Avocent®

MergePoint™ 5224/5240

Installer and Administrator Guide

USA Notification

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Safety and EMC Approvals and Markings

FCC Class A; EN55022 Class A/CISPR 22 Class A; EN55024/CISPR 24 (EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN 61000-4-6, EN 61000-4-11); EN60950/IEC60950-Compliant; CSA Listed (USA and Canada); CE Marking (Europe)

MergePoint™ 5224/5240 Service Processor Manager

Installer and Administrator Guide

Avocent, the Avocent logo, The Power of Being There, Cyclades, MergePoint and DSView are trademarks or registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners.

© 2007 Avocent Corporation. All rights reserved. 590-679-501A

Instructions

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Dangerous Voltage

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Power On

This symbol indicates the principal on/off switch is in the on position.

Power Off

This symbol indicates the principal on/off switch is in the off position.

Protective Grounding Terminal

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

TABLE OF CONTENTS

List of Figures ..... **ix**

List of Tables ..... **xi**

Chapter 1: Installation Introduction **1**

MergePoint 5224/5240 SP Manager Connectors *1*
LEDs *3*
Modem Types and Options *4*
Power Management Unit Options *4*
Safety Precautions and Other Requirements *4*

Chapter 2: Basic Installation Procedures **7**

Supplied with the MergePoint 5224/5240 SP Manager *8*
Rack Mounting the MergePoint 5224/5240 SP Manager *8*
Making Public Ethernet Connections *9*
Connecting Devices *10*
Connecting to a Power Source and Powering Up *10*
Methods for Enabling Web Manager Access *12*
Connecting a Terminal to Configure Basic Network Parameters *13*
Enabling Access to the Web Manager *13*
Changing the root User's Password *15*
Selecting a Security Profile, Adding Users and Configuring Target Devices Using the Web Manager *16*

Chapter 3: Advanced Installation Topics and Tasks **17**

Installing PC Cards in the Front Card Slots *17*
Connecting an External Modem to the AUX Port *18*
Connecting One or More IPDUs to the AUX Port *19*

Chapter 4: Administration Introduction **21**

Overview of MergePoint 5224/5240 SP Manager Features for Administrators *21*
MergePoint 5224/5240 SP Manager Authentication Options *22*
One-time Password Authentication on the MergePoint 5224/5240 SP Manager *24*
User and Group Configuration *25*

Security Profiles *25*
Services *27*
Telnet on the MergePoint 5224/5240 SP Manager *28*
Telnet service configuration *28*
Telnet client configuration *28*
HTTPS on the MergePoint 5224/5240 SP Manager *28*
DHCP on the MergePoint 5224/5240 SP Manager *28*
DHCP client *28*
DHCP server *29*
SNMP on the MergePoint 5224/5240 SP Manager *29*
VPN on the MergePoint 5224/5240 SP Manager *33*
IPSec VPN connections *34*
PPTP VPN connections *36*
DirectCommand on the MergePoint 5224/5240 SP Manager *38*
Message Logging (With Syslog) on the MergePoint 5224/5240 SP Manager *38*
Message filtering levels *38*
Syslog servers *39*
Tasks for configuring syslog messages *39*
Ethernet Ports on the MergePoint 5224/5240 SP Manager *39*
Private Ethernet ports *39*
Public Ethernet ports *39*
Failover *39*
Ethernet media configuration *40*
Dial-in and Callback Access *41*
Power Management Options *43*
Adding Options to the User's Console Login Menu *43*
Routing on the MergePoint 5224/5240 SP Manager *43*
MergePoint 5224/5240 SP Manager Notifications *43*
MergePoint 5224/5240 SP Manager Sensor Alarms *44*
Target Device Configuration *45*
Preparing an addressing scheme *46*
Parameters for configuring target devices *47*
Configuring new target device types *49*
Private Subnets and Virtual DNAT Networks on the MergePoint 5224/5240 SP Manager *50*
Configuring private subnets *50*

Configuring virtual networks (DNAT) *52*
Tasks for configuring IP addresses *52*
Data Buffering on the MergePoint 5224/5240 SP Manager *52*
Firewall/Packet Filtering on the MergePoint 5224/5240 SP Manager *53*
Chains *53*
Rules *54*
Add rule and edit rule options *54*
Tasks for administering packet filtering *55*
How Configuration Changes Are Handled *55*

Chapter 5: Using the Web Manager 57

Features of Administrative Users' Screens *58*
Dialogs in the Web Manager *59*
Web Manager Wizard *60*
Changing the Administrative User's Password in the Wizard *61*
Selecting a Security Profile in the Wizard *61*
Configuring Network Interfaces in the Wizard *62*
Configuring routes *62*
Configuring failover *62*
Configuring primary and secondary Ethernet ports *62*
Configuring Subnets and Virtual (DNAT) Networks in the Wizard *63*
Configuring Target Devices in the Wizard *65*
Configuring Regular Users in the Wizard *66*
Web Manager Access Menu Options for Administrative Users *67*
Accessing the MergePoint 5224/5240 SP Manager Console through the Web Manager *67*
Upgrading IPDU Software *68*
Configuring the AUX Port *69*
Configuring IPDU Power Management *70*
Configuring Over Current Protection for an IPDU *71*
Configuring Users to Manage Power Outlets on an IPDU *71*
Configuring Names and Power Up Intervals for IPDU Outlets *72*
Configuring PC Cards *72*
Configuring System Date and Time *74*
Configuring Boot Characteristics *75*
Local boot options *75*

Network boot options *76*
Configuring Outbound Email *77*
Configuring an Alternate Help File Location *78*
Configuring Target Devices *79*
Adding a target device *79*
Configuring Target Device Types *80*
Configuring Users and Groups *81*
Configuring Device Groups *83*
Configuring Authentication Servers *83*
Configuring a Kerberos authentication server *84*
Configuring an LDAP authentication server *85*
Configuring a NIS authentication server *86*
Configuring a RADIUS authentication server *87*
Configuring an SMB authentication server *88*
Configuring a TACACS+ authentication server *89*
Prerequisites for a TACACS+ server configuration *89*
Configuring an Authentication Method for the MergePoint 5224/5240 SP Manager *90*
Configuring Notifications *90*
Configuring SNMP trap notifications *91*
Configuring pager notifications *92*
Configuring email notifications *93*
Configuring Sensor Alarms *93*
Configuring a syslog message sensor alarm action *94*
Configuring the SNMP trap sensor alarm action *94*
Configuring a pager sensor alarm action *95*
Configuring an email sensor alarm action *96*
Configuring SNMP *96*
Configuring Logging of System Messages (Syslogs) *99*
Configuring the Event Log Backend *100*
Selecting or Configuring a Security Profile *100*
Configuring Network Interfaces *101*
Configuring primary and secondary Ethernet ports *101*
Configuring Firewall Rules for Packet Filtering *102*
Configuring Hosts *103*
Configuring Static Routes *104*

Configuring VPN Connections *104*
Configuring Private Subnets and Virtual Networks *106*
Viewing Status Information about Active Sessions *107*
Viewing System Information *107*
Viewing Information about Detected Devices *107*
Backing Up or Restoring Configuration Files *107*
Upgrading MergePoint 5224/5240 SP Manager Firmware *108*
Restarting the MergePoint 5224/5240 SP Manager *110*

Chapter 6: Administration Tasks Not Performed in the Web Manager 111

Configuring Storage of Buffered Data *111*
Using MindTerm to Create an SSH Tunnel *113*
Specifying the Location for the OTP Databases *114*
How Users are Registered with OTP and Obtain OTP Passwords *116*
Replacing the Self-Signed Certificate With an SSL Certificate for HTTPS *119*
Configuring the DHCP Server *120*
Configuring Dial-ins Using cli *122*
Configuring the Users' Console Login Menu *126*
Configuring Routes With cli *127*
Saving Configuration Changes *128*
Backing Up Configuration Files *129*
Restoring Backed Up Configuration Files *129*
Restoring Factory Default Configuration Files *130*
Adding New Files to Be Backed Up and Restored *130*
Changing Web Manager Time-outs *131*
Changing the Sort Order of Device Listings *132*
Configuring Groups for Use with Authentication Servers *133*
Configuring group authorization for LDAP authentication *133*
Configuring group authorization for RADIUS authentication *136*
Configuring group authorization for TACACS+ authentication *139*

Chapter 7: Using the cli Utility 143

cli Utility Overview *143*
Execution Modes *143*
Command line mode *143*
Interactive mode *144*

Batch mode *144*
cli Options *144*
cli Parameters and Arguments *145*
Entering values with parameters *146*
Entering a command in interactive mode *146*
Entering a command in command code *146*
Entering a command in batch mode *146*
Autocompletion *148*
cli Commands *149*
add *149*
cd *152*
commit *153*
delete *153*
get | show *154*
list *155*
quit | exit *155*
quit! *156*
rename *156*
revert *156*
set *157*
shell *157*
version *157*
Summary of How to Configure the Top Level Parameters *158*

Appendices 165

Appendix A: Troubleshooting *165*
Appendix B: Technical Specifications *168*
Appendix C: Target Device Configuration *169*
Appendix D: Advanced Boot and Backup Configuration *200*
Appendix E: Technical Support *208*

Index 209

LIST OF FIGURES

Figure 1.1: SP Manager Front With PCMCIA Card Slots and Two AC Power Inlets *1*
Figure 1.2: SP Manager Rear With Ethernet, AUX and Console Ports *2*
Figure 1.3: LEDs for Public and Private Ethernet Ports, AUX and Console Ports (Rear) *3*
Figure 2.1: Basic Installation Connections Illustrated *7*
Figure 2.2: Bracket Mounting Holes on the Right Side *8*
Figure 2.3: Wiring the DC Power Terminal to Positive and Negative DC Power Connectors *11*
Figure 2.4: Wiring the DC Power Terminal to Ground *12*
Figure 3.1: Connecting an External Modem to the AUX Port and to the Telephone Network *18*
Figure 4.1: Recommended Target Device Configuration *46*
Figure 4.2: IP Addressing Example *47*
Figure 5.1: Administrative User Options on the Web Manager *58*
Figure 5.2: Example Dialog: Devices Configuration in Wizard Mode *59*
Figure 5.3: MergePoint 5224/5240 SP Manager Configuration Wizard Screen *60*
Figure 5.4: Wizard Confirm Changes Screen *60*
Figure 5.5: Mgmt - Firmware Upgrade Screen With Net Boot Message *109*
Figure 6.1: MindTerm Basic Tunnels Setup Dialog Box *114*
Figure 7.1: Example Branch in the cli Parameter Tree *145*
Figure C.1: Example 1: Private Subnet *184*
Figure C.2: Example 2: Two Private Subnets *186*
Figure C.3: Example 3: Virtual Network Configuration *194*
Figure D.1: Boot Partitions *201*

LIST OF TABLES

Table 1.1: MergePoint 5224/5240 SP Manager Models *1*
Table 1.2: Ports on the Rear *2*
Table 1.3: LED Descriptions *3*
Table 2.1: Methods for Enabling Web Manager Access *12*
Table 4.1: Supported Authentication Types *22*
Table 4.2: User Configuration Settings *25*
Table 4.3: Default Security Profile Services/ Features *26*
Table 4.4: Services Requiring and Not Requiring Additional Configuration *27*
Table 4.5: Values for Configuring SNMP *31*
Table 4.6: Values for Configuring SNMP Views *32*
Table 4.7: Values for Configuring an SNMP Trap Notification *32*
Table 4.8: VPN Client System Requirements and Limitations *34*
Table 4.9: IPSec VPN Configuration Information for Administrators and Users *34*
Table 4.10: Fields for Configuring a PPTP Profile *37*
Table 4.11: Network Interfaces Configuration Values *40*
Table 4.12: Ethernet Port Settings *41*
Table 4.13: Modem and Phone Card Field and Menu Options *42*
Table 4.14: Values for Configuring Sensor Alarms *45*
Table 4.15: Target Device Configuration Parameters *47*
Table 4.16: Values for Configuring Target Device Types *49*
Table 4.17: Fields on the Private Subnet Configuration Dialog *51*
Table 4.18: Values for Configuring Virtual Networks *52*
Table 4.19: Filter Options for Packet Filtering Rules *54*
Table 5.1: Boot Configuration Fields and Options *76*
Table 5.2: Values for Configuring Any Type of Notification *90*
Table 5.3: Fields for Configuring a Pager Notification *92*

Table 5.4: Fields for Configuring an Email Notification *93*
Table 5.5: Fields for Configuring Pager Sensor Alarms *95*
Table 5.6: Fields for Configuring Email Sensor Alarms *96*
Table 5.7: Fields and Menus for Configuring Static Routes *104*
Table 5.8: Information on the Info - Detected Devices Screen *107*
Table 5.9: Firmware Upgrade Screen Fields *108*
Table 6.1: Configuration Files Used in Data Buffering *111*
Table 6.2: Required Information When Creating an SSL Certificate Request *119*
Table 6.3: Web Manager Time-out-related cli Parameters *131*
Table 6.4: Examples of Web Manager Time-out-related cli Parameter Settings *131*
Table 6.5: Methods for Configuring the TACACS+ Authentication Server for Raw Access *139*
Table 7.1: cli Utility Options *144*
Table 7.2: Parameters That Work With the cli add Command *151*
Table 7.3: Setting Top Level cli Parameters *158*
Table B.1: MergePoint 5224/5240 SP Manager Specifications *168*
Table C.1: Default Family Names and Corresponding Expect Script Names *170*
Table C.2: Expect Script Exit Codes *172*
Table C.3: Default Command Templates *173*
Table C.4: Tasks for Creating Addresses to Assign to Target Devices *180*
Table C.5: IP Address Ranges Reserved for Internal Network Addressing *181*
Table C.6: Values for Configuring a Private Subnet *183*
Table C.7: Information Defining a Virtual (DNAT) Network *192*
Table D.1: Options for the create_cf Command *206*

CHAPTER 1

Installation Introduction

This chapter describes the available models, the private and public Ethernet ports, LEDs, power connectors and all other connectors on the MergePoint™ 5224/5240 service processor (SP) manager and provides additional prerequisite information useful throughout this guide.

MergePoint 5224/5240 SP Manager Connectors

The MergePoint 5224/5240 appliance is a 1U service processor manager that serves as a single access point for administering the following types of target devices:

- Servers that have SPs with dedicated Ethernet ports
- Other devices with dedicated Ethernet ports that provide redirected console access

Figure 1.1 illustrates the front of a MergePoint 5240 model SP manager with two AC universal power inlets. The MergePoint 5224 model SP manager front is the same except for the model number.

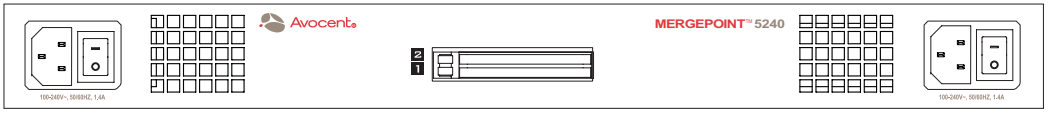

Figure 1.1: SP Manager Front With PCMCIA Card Slots and Two AC Power Inlets

All models have two PCMCIA card slots for connecting PC cards for remote access and storage, as shown in Figure 1.1.

Other models are available with either one AC power supply or two DC power supplies. DC models with two power supplies have terminal blocks on their fronts.

Table 1.1: MergePoint 5224/5240 SP Manager Models

Model	Power Supplies	Power Type	Private Ethernet Ports
MergePoint 5224 SAC	1	AC	24
MergePoint 5240 SAC	1	AC	40
MergePoint 5224 DAC	2	AC	24

Table 1.1: MergePoint 5224/5240 SP Manager Models (Continued)

Model	Power Supplies	Power Type	Private Ethernet Ports
MergePoint 5240 DAC	2	AC	40
MergePoint 5224 DDC	2	DC	24
MergePoint 5240 DDC	2	DC	40

Figure 1.2 illustrates the rear of a MergePoint 5240 SP manager model with 40 private 10/100 Ethernet ports. Figure 1.2 also shows the two public Ethernet ports and other standard ports on the rear of all models.

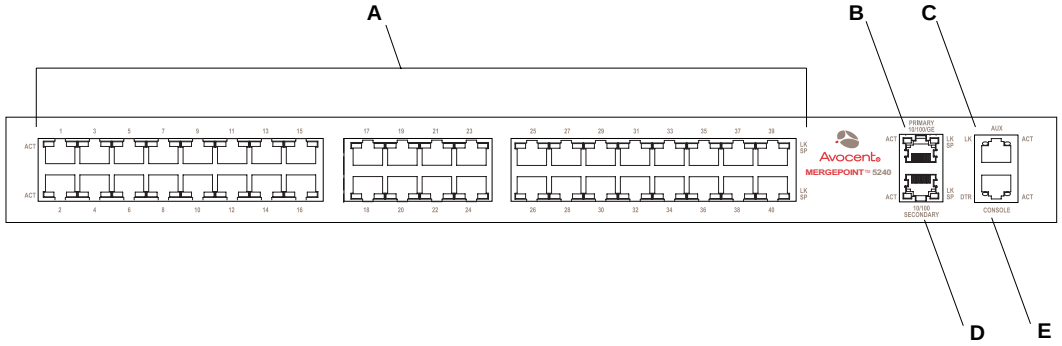

Figure 1.2: SP Manager Rear With Ethernet, AUX and Console Ports

Table 1.2: Ports on the Rear

Letter	Type	Purpose
A	Private Ethernet ports, either 24 or 40.	For connecting SPs and other devices that have dedicated Ethernet ports for management access
B	10/100/GE (Gigabit Ethernet) primary public Ethernet port	For network connection
C	Auxiliary (AUX) port	For connecting an optional modem or Intelligent Power Management Unit (IPDU)
D	10/100 secondary public Ethernet port	(Optional) For connection to a second network connection or for failover connection to the primary network; with Ethernet failover (also known as bonding) enabled, if the primary Ethernet port fails, the secondary one automatically becomes active until the first one recovers
E	Console port	For connecting either a terminal or a computer running a terminal emulation program to enable local administrators and users to use the command line

LEDs

On the rear of the SP manager, two LEDs on each port provide status information about the ports.

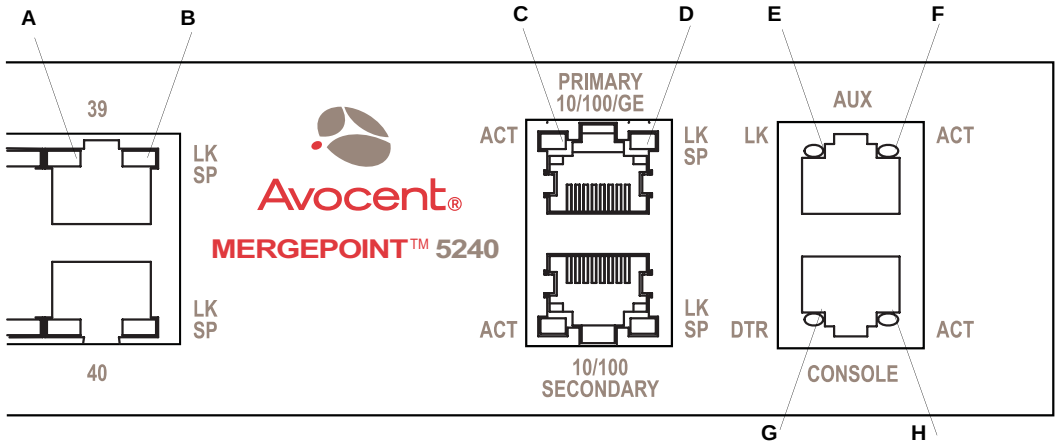

Figure 1.3: LEDs for Public and Private Ethernet Ports, AUX and Console Ports (Rear)

Table 1.3: LED Descriptions

Label	Label	Function	Color/Status
A and C (the left LED on all Ethernet ports)	ACT	Monitor Ethernet activity	• OFF – Indicates no activity. • Green – Blinks for any activity.
B and D (the right LED on all Ethernet ports)	LK/SP	Monitor Ethernet link and speed	• OFF – Indicates either link is not up or cable is not connected. • Green – Indicates the speed is 100 or 1000 Megabits/second. • Yellow – Indicates the speed is 10 Megabits/second.
E	LK	Monitor RS-232 link	• OFF – Indicates either link is not up or cable is not connected. • Green – Lights solid when the link is up and blinks when activity occurs, with frequency proportional to traffic.
F and H	ACT	Monitor RS-232 async activity	• OFF – Indicates no data activity. • Green – Blinks when data is either being received (RX) or transmitted (TX).
G	DTR	Monitors console port for transmissions	• OFF – Indicates the SP manager is not ready to communicate. • ON – Indicates the SP manager is ready to communicate.

Modem Types and Options

Modems can be connected to the MergePoint 5224/5240 SP manager in one of the two following ways:

- An external modem can be connected to the AUX port on the back
- A PC modem card can be inserted into a PCMCIA slot on the front

Power Management Unit Options

Cyclades® Power Management (PM) Intelligent Power Distribution Units (IPDUs) can be connected to the AUX port on a MergePoint 5224/5240 SP manager. Any combination of models of Cyclades PM IPDUs can be daisy-chained to support management of up to 128 outlets.

After an IPDU is connected to the AUX port, AC-powered devices of any type can be plugged into the IPDU. Authorized users can remotely manage power for the target devices after the administrator performs the following tasks:

- Configures the AUX port for power management
- Configures the outlets on connected IPDUs by specifying names to identify devices that are plugged into the outlets
- Authorizes users to power up and down devices connected to IPDU outlets

The administrator may also configure notifications of over-current states to be sent as alarms to specified users.

Safety Precautions and Other Requirements

Failure to observe the precautions in this section may result in personal injury or damage to equipment.

Observe the following general safety precautions when setting up and using Avocent equipment.

- Follow all cautions and instructions marked on the equipment.
- Follow all cautions and instructions in the installation documentation or on any cautionary cards shipped with the product.
- Do not push objects through the openings in the equipment. Dangerous voltages may be present. Objects with conductive properties can cause fire, electric shock or damage to the equipment.
- Do not make mechanical or electrical modifications to the equipment.
- Do not block or cover openings on the equipment.
- Chose a location that avoids excessive heat, direct sunlight, dust or chemical exposure, all of which can cause the product to fail. For example, do not place an Avocent product near a radiator or heat register, which can cause overheating.

- Connect products that have dual power supplies to two separate power sources, for example, one commercial circuit and one uninterruptible power supply (UPS). The power sources must be independent of each other and must be controlled by separate circuit breakers.
- For products that have AC power supplies, ensure that the voltage and frequency of the power source match the voltage and frequency on the label on the equipment.
- Products with AC power supplies have grounding-type three-wire power cords. Make sure the power cords are plugged into single-phase power systems that have a neutral ground.
- Do not use household extension power cords with Avocent equipment because household extension cords are not designed for use with computer systems and do not have overload protection.
- Make sure to connect DC power supplies to a grounded return.
- Ensure that air flow is sufficient to prevent extreme operating temperatures. Provide a minimum space of 6 inches (15 cm) in front and back for adequate airflow.
- Keep power and interface cables clear of foot traffic. Route cables inside walls, under the floor, through the ceiling or in protective channels or raceways.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within specified cable length limitations.
- Leave enough space in front and back of the equipment to allow access for servicing.

When installing Avocent equipment in a rack or cabinet, observe the following precautions:

- Ensure that the floor's surface is level.
- Load equipment starting at the bottom first and fill the rack or cabinet from the bottom to the top.
- Exercise caution to ensure that the rack or cabinet does not tip during installation and use an anti-tilt bar.

When using a desk or table, observe the following precautions:

- Choose a desk or table sturdy enough to hold the equipment.
- Place the equipment so that at least 50% of the equipment is inside the table or desk's leg support area to avoid tipping of the table or desk.

CHAPTER 2

Basic Installation Procedures

This chapter describes basic installation of the MergePoint 5224/5240 SP manager, including how to assign it an IP address needed for remote configuration or for access to connected target devices.

Figure 2.1 illustrates one possible configuration for a 40 port model with one power supply.

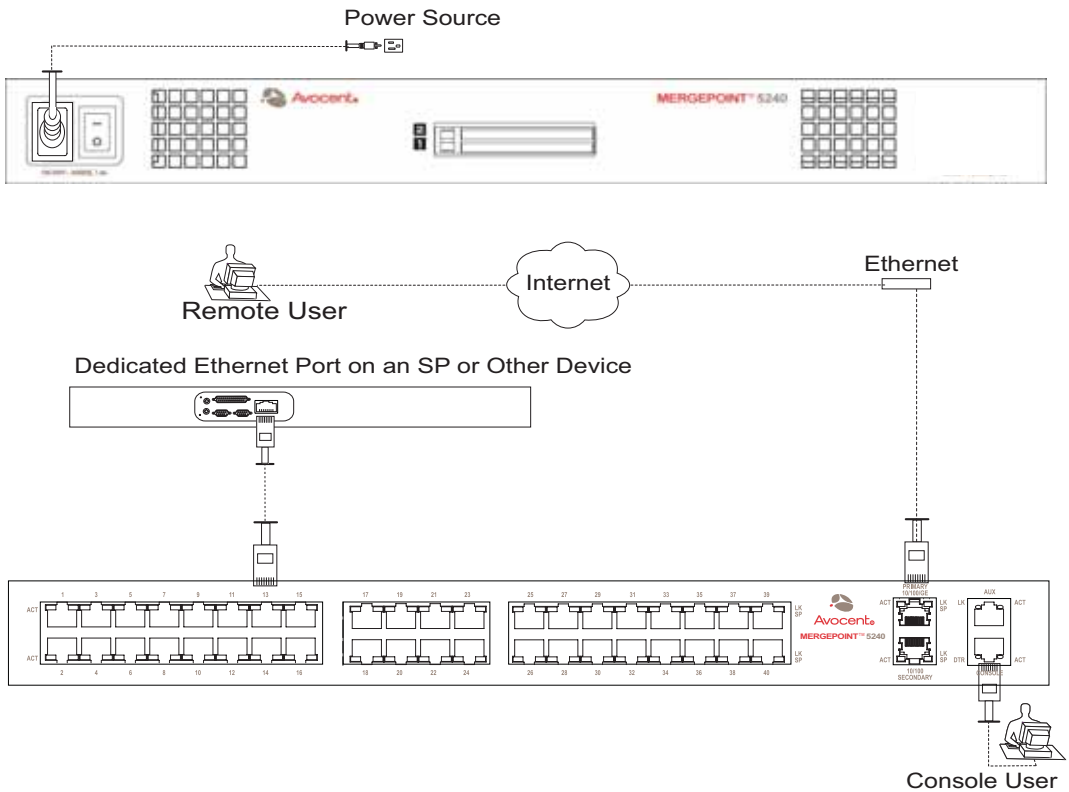

Figure 2.1: Basic Installation Connections Illustrated

CAUTION: Before you start installation, make sure you review and follow the safety precautions listed in *Safety Precautions and Other Requirements* on page 4.

For how to perform optional advanced procedures (connecting PC cards, IPDUs and external modems), see Chapter 3.

Supplied with the MergePoint 5224/5240 SP Manager

Before installing the MergePoint 5224/5240 SP manager, refer to the following list to ensure you have all items that come with the SP manager.

- MergePoint 5224/5240 Service Processor Manager Quick Installation Guide
- Two rack mounting brackets and eight screws
- For AC models, an AC power cable
- RJ-45 to RJ-45 7 ft CAT 5 cable
- DB-9 female to RJ-45 6 ft crossover cable

Rack Mounting the MergePoint 5224/5240 SP Manager

You can rack mount the MergePoint 5224/5240 SP manager either at the front or the rear of a rack or cabinet. Observe all safety precautions described in *Safety Precautions and Other Requirements* on page 4, especially making sure to load the rack from the bottom up.

Before you start, make sure you have the following:

- The two brackets and the eight Phillips screws that are shipped with the SP manager
- A Phillips screwdriver
- Appropriate nuts and bolts for attaching the brackets to the rack

Decide whether to mount the unit on the front or rear and locate the appropriate sets of holes on the sides. The locations of the holes for front (A) and rear mounting (B) are shown in the following figure.

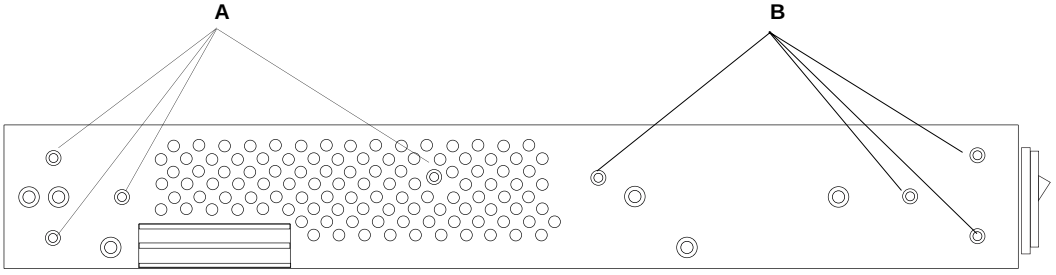

Figure 2.2: Bracket Mounting Holes on the Right Side

To rack mount the SP manager:

1. Attach the right bracket to the right side and the left bracket to the left side.
   a. For each bracket, insert four screws through the bracket's holes into the appropriate holes at either the front or rear.
   b. Use a Phillips screwdriver to tighten the screws.
2. Use the appropriate mounting hardware to mount the SP manager to the rails.

Making Public Ethernet Connections

The primary public Ethernet port must be connected to an Ethernet switch, router or local area network (LAN) that provides Internet access, to enable remote configuration and remote access to target devices.

The secondary public Ethernet port can be optionally used in the following ways:

- To connect to a second network
- To connect to the same network as the primary Ethernet port for redundancy in case of failure of the primary port (Ethernet failover or bonding)

  With a failover configuration, the administrator must take additional steps to enable failover. For more information, see *Public Ethernet ports* on page 39.

One or more optional Ethernet PC cards may be inserted and configured to support the following:

- A second, third or fourth network (depending on how the two public Ethernet ports are configured)
- If failover is configured, a second, third or fourth failover interface

You can use the RJ-45 to RJ-45 Ethernet CAT 5 cable shipped with the SP manager or an off-the-shelf CAT 5 or greater cable (such as CAT 5e) to connect the Ethernet ports to Ethernet switches, routers or local area network (LAN) ports.

To make a public Ethernet connection:

1. Connect one end of a standard Ethernet cable to an Ethernet switch, router or LAN port.
2. If you are making one Ethernet connection, connect the other end of the cable to the primary Ethernet port on the SP manager.
3. If you are setting up Ethernet failover, connect a second cable from the same network to the secondary Ethernet port.
4. If you are using an optional Ethernet PC card on the SP manager, connect a cable between one of the Ethernet connections listed in step 1 to the PC card.

Connecting Devices

The 24 or 40 Ethernet ports on the left side of the rear of the MergePoint 5224/5240 SP manager are for private connections to SPs or other devices.

CAUTION: To comply with FCC and CE certification requirements, use shielded cables when connecting devices to the private Ethernet ports.

To prepare to connect devices:

1. Make sure all configuration is complete on devices to be connected.
2. For the device to use remote authentication, make sure that the following prerequisite configuration is complete:
   - Authentication servers are installed and fully configured
   - You have obtained from each authentication server's administrator the information (such as the IP address), which is needed to configure the authentication server on the SP manager

NOTE: After the SP manager is installed, make sure to configure the desired authentication method for each device, unless authentication is being managed by DSView 3 management software.

To connect devices to the private Ethernet ports:

Connect a standard Ethernet cable from the private Ethernet ports on the SP manager to any of the following types of Ethernet ports on the other end:

- A dedicated Ethernet port on an SP
- A dedicated Ethernet port on a router or other device that gives access to the device's console
- A switch that is connected to multiple devices (not recommended)
- A dedicated Ethernet port on a blade managing multiple SPs

Connecting to a Power Source and Powering Up

When the MergePoint 5224/5240 SP manager has two power supplies, connect each power supply to a separate power source for redundancy in case one power source fails. The power sources must be independent of each other and must be controlled by separate circuit breakers.

To connect AC power inlets to an AC power source and power up:

1. Make sure the SP manager's power switch(es) are off.
2. Plug the power cord(s) into the SP manager and plug the other end(s) into an appropriate grounded power source(s).

NOTE: On dual AC models, plug the power cords into separate power sources.

3. Power up the SP manager.

To connect DC power terminal blocks to a DC power source and power up:

1. Make sure the SP manager's power switch(es) are off.
2. Perform the following steps twice to wire both terminal blocks to independent power sources.
   a. Loosen the hex screw labeled RTN, attach the red wire (positive) from the DC power supply to the screw and tighten the screw again.
   b. Loosen the hex screw labeled -48VDC, attach the black wire (return) from the DC power supply to the screw and tighten the screw again.

      Figure 2.3 illustrates the red wire connected between the positive connector and the RTN screw and the black wire connected between the negative connector and the -48VDC screw.

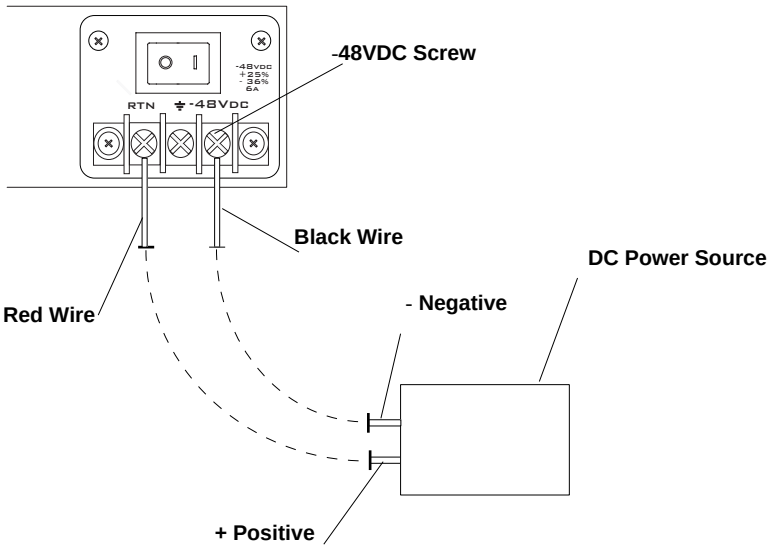

Figure 2.3: Wiring the DC Power Terminal to Positive and Negative DC Power Connectors

   c. Loosen the hex screw labeled with the ground symbol, attach a green grounded wire to the screw and tighten the screw again.

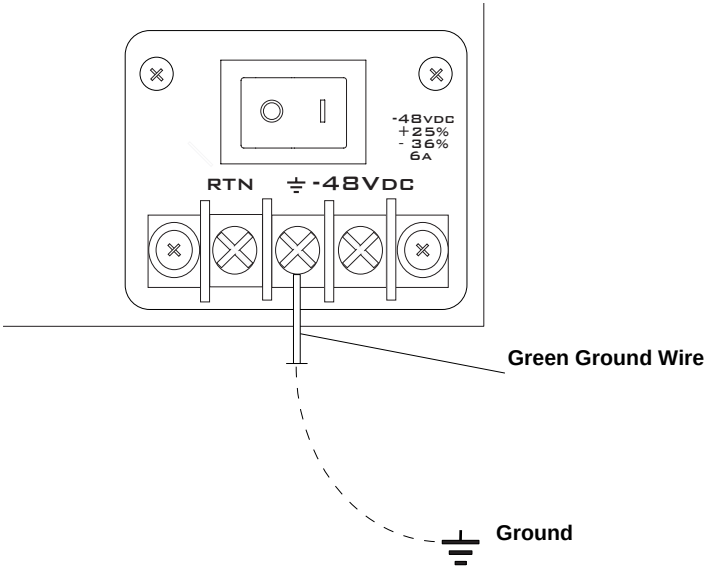

Figure 2.4: Wiring the DC Power Terminal to Ground

3. Power up the SP manager.

Methods for Enabling Web Manager Access

An administrator who knows the password for an administrative user account and who has network access to the MergePoint 5224/5240 SP manager must enter the SP manager's DNS name or IP address in a browser to bring up the Web Manager and to finish the configuration of users and connected target devices.

Perform one of the tasks in the following table to set a static IP address or set up a DHCP server, so that the basic network configuration can be done to enable the administrative user to use the Web Manager to finish configuration.

Table 2.1: Methods for Enabling Web Manager Access

Method	Considerations	Where Described
Connect a terminal to the console port and use the cli command to assign a static IP address.	You must be at the same location as the SP manager to make the local connection.	*Connecting a Terminal to Configure Basic Network Parameters* on page 13
Use the DHCP-assigned address.	DHCP is enabled by default. It relies on a DHCP server that must be available to the SP manager.	*To use a dynamic IP address to access the Web Manager:* on page 14

Table 2.1: Methods for Enabling Web Manager Access (Continued)

Method	Considerations	Where Described
Use the default IP address 192.168.160.10 to bring up a Web Manager to set a fixed IP address.	You must temporarily change the network portion of the IP address of a computer on the same subnetwork to be able to use the default IP address in launching the Web Manager.	*To use a dynamic IP address to access the Web Manager:* on page 14

Connecting a Terminal to Configure Basic Network Parameters

If you connect a terminal or workstation to the console port, you can use the cli utility to configure basic network parameters as described in *To configure basic network parameters using a terminal:* on page 14.

Perform the following steps to connect a terminal or a workstation to the console port. If connecting a PC, make sure that HyperTerminal or another terminal emulation program is installed on the Windows operating system. On a workstation running a UNIX-based operating system, such as Linux or Solaris, make sure that a compatible terminal emulator such as Kermit or Minicom is installed.

This procedure assumes you have the RJ-45 to DB-9 6 ft CAT 5 cable shipped with the SP manager or an off-the-shelf equivalent CAT 5 or greater cable. If the terminal or workstation has a USB port, you also need a USB to DB-9 converter.

NOTE: Only use a crossover cable.

To connect a terminal to the console port:

1. If connecting to a workstation or terminal with a DB-9 male port, perform these steps.
   a. Connect the RJ-45 end of the cable to the console port.
   b. Connect the DB-9 male end of the cable to the DB-9 connection on the terminal or workstation.
2. If connecting to a workstation or terminal with a USB port, perform these steps.
   a. Connect the RJ-45 end of the cable to the console port.
   b. Connect the DB-9 female end to the DB-9 male end of a USB converter.
   c. Connect the USB end of the converter to a terminal or workstation.

Enabling Access to the Web Manager

Perform the procedures in this section to enable a remote administrator to finish configuration using the Web Manager. These procedures require a terminal or a computer with a terminal emulation program to be physically connected to the console port of the SP manager.

To configure basic network parameters using a terminal:

1. Using either a terminal or a terminal emulation program installed on a computer that is connected to the SP manager, start a session with the following console port settings: Serial Speed: 9600 bps, Parity: None, Flow Control: None, Data Length: 8 bits, Stop Bits: 1 and ANSI emulation.
2. Log into the console port as the root user with the default password **cyclades**.

CAUTION: For security, change the default password for the root user immediately.

3. Enter the **passwd** command, and enter and confirm a new password when prompted.

   ```
   [root@MergePoint5224 /]# passwd
   ```

4. Invoke the **cli** utility.

   ```
   [root@MergePoint5224 /]# cli
   ```

5. Make sure the primary Ethernet interface (eth0) is active, then set the method to static, assign a static IP address, a gateway and a netmask.

   ```
   cli> set network interface eth0 active yes method static address
   SPmanager_IPaddress gateway gateway_IP_address netmask netmask
   ```

6. Specify a hostname, a domain, a DNS server IP address, and an optional secondary DNS server IP address.

   ```
   cli> set network hostname SP manager_name resolv domain domain_name
   dns0 DNS_server_IPaddress dns1 secondary_DNS_server_IPaddress
   ```

7. Confirm the configuration for the interface.

   ```
   cli> get network interface eth0
   ```

8. Confirm the name server configuration.

   ```
   cli> get network resolv
   ```

9. Save the changes.

   ```
   cli> commit
   ```

10. Exit from the cli utility.

    ```
    cli> quit
    ```

11. Log out and enter the IP address in a browser to bring up the Web Manager to add users and configure access to target devices as desired.
12. Finish configuring security, users and target devices on the SP manager using the Web Manager.

To use a dynamic IP address to access the Web Manager:

This procedure assumes that DHCP is enabled and that you know the IP address that is currently assigned to the SP manager from a DHCP server on the same subnet.

1. Use the SP manager's dynamically assigned IP address in a browser to bring up the Web Manager.
2. Finish configuring target devices, users, and other SP manager parameters using the Web Manager.
3. Make sure that the root user changes the password by logging into the SP manager console. See *To change root's password:* on page 15.

To use the default IP address to access the Web Manager:

NOTE: The default IP address for the MergePoint 5224/5240 SP Manager is 192.168.160.10. This procedure assumes that you are able to temporarily change the IP address of a workstation that is on the same subnet as the SP manager.

1. On a computer with a physical network connection to the SP manager, change the network portion of the IP address of that computer to 192.168.160 and make sure that the host portion of the IP address is not the same as that of the SP manager.
2. Bring up a browser on the computer whose address you changed, enter the SP manager's default IP address (http://192.168.160.10) to bring up the Web Manager, and log in.
3. To allow subsequent use of the Web Manager from any computer, click the *Wizard* button and select the *Network Settings* option to change the SP manager's IP address to a fixed public IP address and to configure the other basic network parameters.
4. Restore the computer's previous IP address.

Changing the root User's Password

Whatever method is used to enable access to the Web Manager, the root user must always log into the console and change the password from the default. The admin user cannot change the root user's password, and the root user cannot log into the Web Manager to change the root password. The following options are available:

- Until an IP address is available for the MergePoint 5224/5240 SP manager, the only way that the root user can change the root password is to log in locally through the console port. See *To configure basic network parameters using a terminal:* on page 14.
- After an IP address is available for the SP manager, the remote root user can use ssh to connect to the console and log in from a remote location and change the password.

To change root's password:

1. Use SSH to connect to the console using the SP manager's IP address or DNS name.
2. When prompted, login as root.

   The default password is cyclades.

   login as: root

   Sent username "root"

root@172.26.31.222's password: cyclades

3. Enter the **passwd** command, and enter and confirm a new password when prompted.

```
[root@MergePoint5224 /root]# passwd
```

Selecting a Security Profile, Adding Users and Configuring Target Devices Using the Web Manager

For the configuration tasks the administrator must perform, see Chapter 4. These tasks include selecting a security profile, adding users and configuring target devices.

For information on how MergePoint 5224/5240 SP manager administrators and users access the SP manager and perform management actions on target devices, see the MergePoint 5224/5240 Service Processor Manager User Guide.

CHAPTER 3

Advanced Installation Topics and Tasks

Installing PC Cards in the Front Card Slots

Two PC cards of different types can be installed in any order. Two PC cards of the same type, however, must be installed with the card in slot 1 configured first, followed by the card in slot 2.

To avoid the risk that swapping in a new PC card may result in the configuration being lost on one or both of the cards, follow the procedure under *To swap in a new PC card:* on page 17 to remove any existing cards then insert and configure the new card before reinserting and reconfiguring the old card. Supported cards are listed at: http://www.avocent.com on the product page.

To install a PC card:

NOTE: Some cards take up both card slots.

1. Insert a PC card into a front slot(s) and slide the card in until it is firmly seated.
2. Use the Web Manager - Settings - PCMCIA form to configure the PC card.
   a. Click the *Insert* button on the form next to the number of the slot where the card is installed. A prompt displays asking if you have inserted the card into the slot.
   b. Click *Yes*.
   c. Click the *Configure* button. A PC card configuration form appears.
   d. Select a card type from the Card Type pull-down menu. Fill out the fields and select among the choices on the menus.

To remove a PC card:

1. On the Web Manager - Settings - PCMCIA form, select the *Eject* button next to the card's slot number.
2. On the front of the SP manager, press the button next to the slot.
3. Remove the card from the slot.

To swap in a new PC card:

Complete the following steps if only one card slot is in use, you wish to replace the current card (or add a new one) and the new card is the same as the one already installed.

1. Eject the card.
2. If only one slot is currently in use, insert and configure the new card.

   -or-

   If both slots are in use, press the buttons next to both slots on the front of the SP manager. Then insert and configure the new card.

Connecting an External Modem to the AUX Port

An external modem can be connected to the AUX port on the back of the SP manager and then connected to the telephone network.

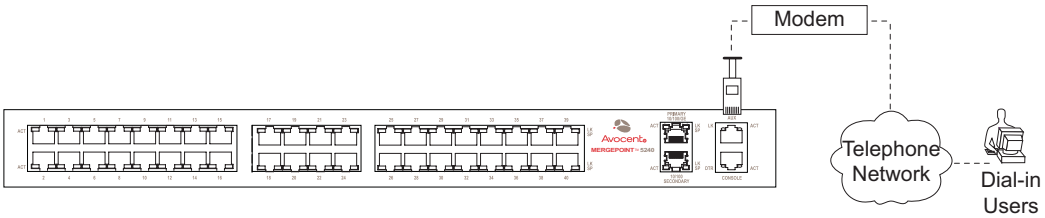

Figure 3.1: Connecting an External Modem to the AUX Port and to the Telephone Network

This procedure requires the following cables and connectors:

- A straight-through CAT 5 or greater cable for connecting the AUX port to the external modem, with an RJ-45 connector on one end and the appropriate connector or adaptor (USB, DB-9 or DB-25) on the other end
- A phone cord (for connecting the modem to a live phone line) with RJ-11 connectors on both ends

To connect an external modem to the AUX port:

1. Connect the RJ-45 end of the cable to the AUX port on the SP manager.
2. Connect the other end of the cable to the modem.
3. Connect the phone cord between the jack on the modem and a live telephone jack at your site.
4. Configure the AUX port for PPP.

   See *To configure the AUX port for IPDU power management:* on page 70 for details.

Connecting One or More IPDUs to the AUX Port

You can daisy-chain any combination of Cyclades PM IPDUs to the AUX port with up to a total of 128 outlets.

This procedure requires the following cables:

- A straight-through RJ-45 to RJ-45 CAT 5 or greater cable for connecting the IPDU to the SP manager and another cable for each IPDU to be daisy-chained

NOTE: Do not plug the SP manager into an IPDU that is connected to the SP manager's AUX port.

To connect an IPDU to the AUX port:

1. Connect one end of the cable to the AUX port.
2. Connect the other end of the cable to the In port of the IPDU.
3. Configure the AUX port for Power Management. See *To configure the AUX port for IPDU power management:* on page 70 for details about configuring the AUX port.

To daisy-chain multiple IPDUs to the SP manager:

1. Connect one end of the cable to the Out port of an IPDU that is already connected to the AUX port.
2. Connect the other end of the cable to the In port of the next IPDU.
3. Repeat steps 1 and 2 until you have connected the desired number of IPDUs.
4. Configure the AUX port for power management. See *Configuring the AUX Port* on page 69.

NOTE: Make sure that all daisy-chained IPDUs are running the same firmware version.

CHAPTER 4

Administration Introduction

An administrator configures the MergePoint 5224/5240 SP manager after installation to set up user authorizations and authentication, and to control access to target devices. An administrator also performs maintenance activities such as upgrading the firmware.

DSView 3 management software, which provides a single interface for controlling multiple appliances, may be purchased separately and installed on a DSView 3 management software server.

After initial installation and configuration, administration is usually performed remotely either through the Web Manager or through DSView 3 management software.

On standalone SP managers not managed by DSView 3 software, Web Manager administration can be performed only by administrative users. Administrative users are those who either know the password for the default admin user account or who have user accounts that are in the admin group.

Users access managed target devices either through the DSView 3 software, the SP manager's Web Manager or SSH. For more background information about types of users and types of access, see the MergePoint 5224/5240 Service Processor Manager User Guide.

Overview of MergePoint 5224/5240 SP Manager Features for Administrators

The MergePoint 5224/5240 SP manager mediates between authorized users (who may be either local or remote users on the public network) and target devices that are connected to the SP manager's private Ethernet ports. Connected target devices are thereby isolated on a private network that cannot be accessed except by going through the SP manager.

Communications between users and the SP manager and through the SP manager to target devices are protected by SSH encryption. Communications between the SP manager and the target devices are proxied and the potentially vulnerable protocols used by most SPs are not exposed on the public network.

Administration of the SP manager is separate from management of the target devices. Multiple authorized users can manage target devices while only administrators can configure access and security on the SP manager.

MergePoint 5224/5240 SP Manager Authentication Options

The administrator can configure many common authentication methods for logins to the SP manager or to target devices. By default, all logins to the SP manager and target devices use Local authentication.

See the authentication-related considerations in the following bulleted list. These authentication methods use both local authentication and authentication servers in the order shown: Local/ AuthType, AuthType/Local and then AuthType/DownLocal.

- The AuthType/Local and AuthType/DownLocal authorization methods are referred to as authentication methods with local fallback options.
- Administrators can specify separate authentication types for SP manager logins and for target devices.
- Local and OTP authentication methods and the authentication methods that have local fallback options require user accounts configured on the SP manager.

If configuring any authentication method other than Local, the administrator user must make sure the SP manager has network access to an authentication server for every authentication method specified.

NOTE: This section discusses only the types of authentication used for controlling who can access the SP manager and target devices. Other authentication methods that are used by SNMP, PPTP, IPSec or PPP are described in the related sections.

NOTE: For Native IP and DirectCommand to work, the authentication method configured for the SP manager must be identical to the authentication method configured for the target device. For example, assigning LDAP to the SP manager and LDAP/Local to the target device causes attempts to achieve Native IP or Device Command access to the target device to fail.

The following table lists the supported authentication methods and indicates which methods are available for the SP manager and which are available for target devices. When a table cell is blank, the authentication method is not supported.

Table 4.1: Supported Authentication Types

Type (name in cli)	Description	SP Manager	Target Device
None	No login required.		X
Local (local)	Uses local user/password for local authentication on the SP manager.	X	X
Kerberos (krb5)	Uses user/password configured on the Kerberos authentication server. No logins allowed if Kerberos server is down or Kerberos authentication fails.	X	X

Table 4.1: Supported Authentication Types (Continued)

Type (name in cli)	Description	SP Manager	Target Device
Kerberos Down/Local	Uses local authentication if Kerberos server is down.	X	X
Kerberos/Local	Uses local authentication if Kerberos authentication fails.	X	X
Local/Kerberos	Uses Kerberos authentication if local authentication fails.	X	X
LDAP (ldap)	Uses user/password configured on the LDAP (Lightweight directory access protocol) authentication server. No logins allowed if LDAP server is down or LDAP authentication fails.	X	X
LDAP Down/Local	Uses local authentication if LDAP server is down.	X	X
LDAP/Local	Uses local authentication if LDAP authentication fails.	X	X
Local/LDAP	Uses LDAP authentication if local authentication fails.	X	X
NIS (nis)	Uses user/password configured on the NIS authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X	X
NIS Down/Local	Uses local authentication if NIS server is down.	X	X
NIS/Local	Uses local authentication if NIS authentication fails.	X	X
Local/NIS	Uses NIS authentication if local authentication fails.	X	X
OTP	Uses the one-time password (OTP) authentication method.		X
OTP/Local	Uses the local password if the OTP password fails.		X
RADIUS (radius)	Uses user/password configured on the RADIUS authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X	X
RADIUS Down/Local	Uses local authentication if RADIUS server is down.	X	X

Table 4.1: Supported Authentication Types (Continued)

Type (name in cli)	Description	SP Manager	Target Device
RADIUS/Local	Uses local authentication if RADIUS authentication fails.	X	X
Local/RADIUS	Uses RADIUS authentication if local authentication fails.	X	X
SMB (smb)	Uses user/password configured on the SMB authentication server (for Microsoft Windows NT/2000/2003 Domain). No logins allowed if SMB server is down or SMB authentication fails.	X	X
SMB Down/Local	Uses local authentication if the SMB server is down.	X	X
SMB/Local	Uses local authentication if SMB authentication fails.	X	X
Local/SMB	Uses SMB authentication if local authentication fails.	X	X
TACACS+ (tacplus)	Uses user/password configured on the Terminal Access Controller Access Control System (TACACS+) authentication server. No logins allowed if NIS server is down or NIS authentication fails.	X	X
TACACS+ Down/Local	Uses local authentication if TACACS+ server is down.	X	X
TACACS+/Local	Uses local authentication if TACACS+ authentication fails.	X	X
Local/TACACS+	Uses TACACS+ authentication if local authentication fails.	X	X

An administrative user can use the Web Manager and any administrator can use the cli utility for configuring an authentication method for the SP manager and target devices and for configuring authentication servers.

One-time Password Authentication on the MergePoint 5224/5240 SP Manager

OPIE (one-time passwords in everything) software (www.inner.netpub/opie) on the SP manager supports the OTP authentication method for certain types of access. This section describes the options the administrator has for configuring OTP authentication.

The root user must perform the initial configuration manually (not through the Web Manager) as described in Chapter 5.

User and Group Configuration

On the MergePoint 5224/5240 SP manager, two user accounts, a normal UNIX user and an SP manager-specific user account (called an spmanager user) are needed to give a user access to the SP manager and to authorize the user for access to management functions on target devices.

Both types of user accounts are created transparently when an administrator adds a user through the Web Manager. When an administrator uses the cli utility, the administrator must take separate steps to add the user both as a regular and spmanager user.

The administrator configures user accounts by assigning parameters that are described in the following table.

Table 4.2: User Configuration Settings

Settings	Notes
Username	Login name required for the user account.
Full name	Administratively defined name to identify the user (the UNIX GECOS).
Password	Password used for accessing the SP manager.
Target Device Access	Select from a list of configured target devices and then configure user access by selecting from the following list of management actions.
• Sensors • Power • Event log • Service Processor Console • Target Device Console • Native IP and DirectCommand	Allow the user to perform the selected management actions on a selected target device. For more details about these actions, see the MergePoint 5224/5240 Service Processor Manager User Guide. **NOTE:** A user is authorized for both Native IP and DirectCommand™ access using the same permission.
PPP/PPTP access • None • PPP (dialup only) • PPTP (VPN only) • PPP (dialup) and PPTP (VPN)	Allow the user to use PPP or PPTP or both for contacting the SP manager. Requires a password, which may be different from the one required to access the SP manager.

The administrator can assign users to a group to make it possible for multiple users to perform management actions on one or more target device.

Security Profiles

Each SP manager has a security profile defined during initial configuration. The type of security profile selected by the administrator controls the following:

- Which services are turned on
- Whether a default authentication is specified for all subsequently configured target devices
- Whether authorizations are checked (bypassing authorizations is not available in any of the default security profiles, but it can be selected in a custom security profile)

The administrative user defines the security profile during initial configuration. The security profile can be changed later. Services can also be turned on and off independently from the security profile. For more details, see *Services* on page 27.

Table 4.3 describes the services that are enabled and disabled in the preconfigured security profiles: moderate, secured and open.

Table 4.3: Default Security Profile Services/ Features

This feature:	Is enabled in this security profile:	Is disabled in this security profile:
HTTP	Moderate, Open	Secured
HTTPS	Moderate, Secured, Open	
ICMP	Moderate, Open	Secured
IPSec	Moderate, Open	Secured
PPTP	Moderate, Open	Secured
RPC	Open	Moderate, Secured
SNMP v1	Open	Moderate, Secured
SNMP v2c	Open	Moderate. Secured
SNMP v3	Open	Moderate, Secured
SSH v1	Open	Moderate, Secured
SSH v2	Secured, Open	Moderate
Telnet to MergePoint 5224/5240	Open	Moderate, Secured
Default authentication type to access target devices set to Local	Moderate, Secured, Open	

If the administrator chooses to configure a custom security profile, the administrator can select among all the options listed in Table 4.3. In addition, the administrator can allow root logins using SSH, redirect HTTP to HTTPs, assign an alternate port to SSH, HTTP or HTTPS or select a default authentication type.

Any default authentication type specified in a custom security profile is selected by default whenever a new target device is configured in the Web Manager. The specified authentication type is also assigned by default to any new target device configured using the cli utility.

The administrative user is always able to change the authentication type for each individual target device.

Services

A network service is available on the SP manager if the security profile enables the service or if the administrator has enabled the service through the Web Manager, cli or regular UNIX commands.

Administrators can turn services on and off by using the Web Manager Config - Services page or by using either the cli utility or regular Linux commands.

In the Web Manager, the security profile screen and the services screen detect when a service is enabled using either the Web Manager or cli utility. If the administrative user unchecks a service in the Config - Services page, the custom security profile screen then shows the service as disabled and vice versa. Similarly, if a service is enabled using either the Web Manager or the cli utility, the cli utility detects it. However, if the root user turns services on and off on the command line using Linux start and stop commands, the change in state for the service is not detected either by the Web Manager or the cli utility.

Table 4.4: Services Requiring and Not Requiring Additional Configuration

Services Requiring Additional Configuration	Services Not Requiring Additional Configuration
DHCP	FTPD
HTTPS	HTTP
IPSec	ICMP
PPTP	INETD
NTP	PMD
SNMP	RPC
Syslog	SSH
Telnet	

Passing SP management commands as parameters to ssh on the command line is always enabled as long as the following are both true:

- The SP supports the command
- The user is authorized to use that command for that SP

Telnet on the MergePoint 5224/5240 SP Manager

Telnet is not encrypted, so the SP manager controls its use to protect communications. By default, the Telnet service is disabled, while a Telnet client is used for proxied communications between users on the public network and target devices on the private network side of the SP manager.

Telnet service configuration

The Telnet service is not supported by any of the default security profiles and telnetd is not active, to prevent users from using Telnet clients from remote workstations either to connect to the SP manager or to connect through the SP manager to target devices. Encrypted SSH clients may be used instead. An administrator can choose to enable the Telnet service. Even if the Telnet service is enabled, the SP manager-specific target device management commands cannot be passed as parameters to the telnet command but only to the ssh command. Chapter 4 describes how to enable the Telnet service.

Telnet client configuration

A Telnet client is used when proxying communications between users and most types of target devices on the private network because all supported target device types support Telnet connections while some do not support SSH. The SP manager uses ipmitool commands for IPMI-type SPs. If an SP must be on the public network, then the administrator should strongly consider configuring an SSH client to be used instead of the Telnet client, if SSH is supported by the SPs. Chapter 4 describes how to configure an SSH client to be used instead of the Telnet client when communicating with SPs.

HTTPS on the MergePoint 5224/5240 SP Manager

For HTTPS (secure HTTP based on SSL) to work, an SSL certificate must be present on the SP manager, so a self-signed certificate is automatically generated. To reduce the risks posed by weaknesses inherent in self-signed certificates, administrators are strongly advised to replace the automatically generated self-signed certificate with an SSL certificate from an official certificate authority (CA). See *To replace the self-signed certificate with one from a certificate authority:* on page 119 for the procedure.

DHCP on the MergePoint 5224/5240 SP Manager

Both a DHCP client and a DHCP server are available on the SP manager.

DHCP client

The SP manager's DHCP client is active, with DHCP enabled by default for the primary Ethernet port. With the default configuration, if the SP manager cannot find a DHCP server on the same subnet, it falls back to using the default IP address.

DHCP server

A DHCP server (dhcpd) is present but disabled on the SP manager by default. The administrator may want to enable the DHCP server to provide fixed IP addresses for connected target devices that are running DHCP client software. The fixed IP addresses use the following DHCP features:

- Persistent leases, which allow the target device on the private side of the SP manager to keep the same IP address even after the SP manager or the target device is rebooted.
- Persistent storage of lease information, with the leases file and the dhcpd configuration files stored in the Flash memory and available to be optionally updated from time to time when dhcpd is enabled.
- Preconfigured leases: using the MAC address of the target device, the administrator can assign an IP address to a client before the SP manager sees the target device on the network.

NOTE: IP addresses assigned to connected target devices must remain constant over time because each target device is assigned an IP address as part of its configuration on the SP manager. For that reason, a DHCP server should not be used to provide dynamic IP addresses to target devices.

The ability of DHCP to supply fixed addresses can be used to implement the addressing scheme for target devices, which is described in *Preparing an addressing scheme* on page 46.

The administrator can enable the DHCP server and assign IP addresses to target devices by logging into the command line as root and manually editing the /etc/dhcpd.conf file and performing other steps described under *Configuring the DHCP Server* on page 120. Before deciding whether to use the DHCP server to configure addresses for target device, the administrator should understand the available options for assigning IP addresses to target devices, which are described in *Address configuration for target devices* on page 180.

SNMP on the MergePoint 5224/5240 SP Manager

The administrator can activate Simple Network Management Protocol (SNMP) agent software that resides on the SP manager. The SNMP agent provides access to the SP manager by an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager and provides proxied access to SNMP data from connected SPs that implement SNMP agents. The SNMP agent can be configured to send notifications (also known as traps) about significant events on the SP manager and on target devices.

The administrator must configure the SNMP agent to use the version of SNMP supported by the management application, either SNMP v1, v2c and v3. The use of v3 is strongly encouraged wherever possible because it provides authentication and encryption of data that is lacking in v1 and v2c.

Access to information provided by the SP manager and its proxied target devices can be obtained in either of the two following ways:

- The recommended access method for agents which support only SNMP version 1 or 2c is through a VPN tunnel to the MergePoint 5224/5240 SP manager. The SP manager provides the

authentication and encryption lacking in those protocol versions. The SNMP management application can then be used to for SNMP management of the target device.

When versions 1 or 2c agents are used to obtain native management access to a target device, no SNMP configuration is needed. Support is implemented entirely through the VPN connection limited by iptables rules that restrict access to particular target devices.

CAUTION: The SNMP daemon, snmpd, running on the SP manager allows access to proxied data using the v1 and 2c protocols without the creation of a VPN tunnel, but the lack of security inherent in these protocols means this option should be used with caution if it is used at all.

- The access method agent which supports version 3 is via a local Net-SNMP daemon. The proxying of traps is not supported by Net-SNMP. Forwarding of traps is supported, with filtering by source address.

If SNMP is used as recommended, no public client is allowed unauthenticated access to either managed clients or to the SP manager itself. For compatibility with other clients, unencrypted transfer of data is possible with SNMP v3 connections, but unencrypted data transfer is strongly discouraged.

User and group information for v3 connections must be different from the user and groupnames used for accessing the SP manager for the following reasons:

- To keep the SP manager user information more secure, since SNMP usernames and passwords are stored in cleartext in /etc/snmp/snmpd.conf
- To allow different users and groupings to be used for SNMP access

The administrator can configure the following:

- General information provided by the SP manager, including location and contact fields
- Who has access to SNMP information
- How traps are handled locally
- Trap forwarding

By default, SP manager traps occur on the following types of events:

- Interface up/down
- PC card insertion/removal
- Power supply events

Traps are handled the three following ways:

- When access is through a VPN tunnel, the public-side computer directly receives SNMP traps from the target device
- SNMP traps can be forwarded to SNMP agents based on the source address of the trap
- Locally, traps are sent to the syslog facility, which may use the information to send notifications

Before enabling SNMP, depending on the version of SNMP in use, the administrator will need some or all of the information in the following table.

Table 4.5: Values for Configuring SNMP

Values	Description
SysContact	Email address of the SP manager administrator
SysLocation	Location of the SP manager
OID	Object Identifier. A unique indentifier for each object in an SNMP MIB. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the Internet Engineering Task Force (IETF), which grants authority for parts of the OID name space to individual organizations. Cyclades has the authority to assign OIDs that can be derived by branching downward from the node in the MIB name tree that starts at 1.3.6.1.4.1.4413.
SNMP version (also called protocol)	• v1 - Uses a community string match for authentication • v2c - Uses a community string match for authentication • v3 - Uses a username for authentication. In addition to the username, an optional authentication password may be used. An encryption password also may be used for encrypting traffic. Cyclades recommends that both authentication and encryption be used to maximize the security of data and commands. Available authentication methods are MD5 or SHA. Available encryption methods are DES and AES.
Community	For SNMP v1 and v2c only the community name is used for authentication. An arbitrary string, with a maximum length of 256 characters. Does not need to match the community name used on the public side or be unique on the private side. Must match the community string expected by the target device, often public.
Source	For SNMP v1 and v2c only. • Default • Use IP - Enter an IP for the source target device in the field if you select this option. If the default is selected, then all traps from all source IPs are forwarded to the destination IP.
For configuring SNMP v3 only:	
Auth Level/Security level	No auth - Applies to v1 and v2c by default and is an option in v3. Auth Auth & crypt
User name	Username to be used for authentication.
Auth method	• MD5 • SHA
Auth pass	Optional password used for authentication. Must be either empty or at least eight characters.

Table 4.5: Values for Configuring SNMP (Continued)

Values	Description
Encryption	• DES • AES
Crypt pass	Optional password used for encryption. Must be either empty or at least eight characters. If used, an authentication password is required.

Strings are defined as case-sensitive ASCII, not beginning with a hash and delimited by a space, form-feed ('\f'), newline ('\n'), carriage return ('\r'), horizontal tab ('\t'), vertical tab ('\v') or null ('\0'). Any character may be included if it is escaped with a backslash ('\'). Two backslashes are interpreted as one.

Views can be created to define sections of an OID tree that are included and excluded from access. When a view is being defined, more than one line can be used to build a view. For example, one line may allow access to a subtree, and another may remove access to a portion of that subtree.

The following table describes the values used for configuring views.

Table 4.6: Values for Configuring SNMP Views

View name	Administratively assigned name
OID: Include or Exclude	Object Identifier. A unique indentifier for each object in an SNMP MIB. The OID naming scheme is in the form of an inverted tree with branches pointing downward. The OID naming scheme is governed by the Internet Engineering Task Force (IETF), which grants authority for parts of the OID name space to individual organizations.
Mask: Include or Exclude	Mask that defines a view subtree. Can be all ones, all zeros or a combination of both. Default = ff.

The following table describes the values used for configuring SNMP traps.

Table 4.7: Values for Configuring an SNMP Trap Notification

For configuring SNMP traps only:	Options
Generic trap type	coldStart warmStart linkDown linkUp authenticationFailure egpNeighbor Loss enterpriseSpecific
Server	The IP address or DNS name of the SNMP manager
Body	The text you want sent in the trap message

See Chapter 4 for the tasks related to administering SNMP on the SP manager.

VPN on the MergePoint 5224/5240 SP Manager

As described in the MergePoint 5224/5240 Service Processor Manager User Guide, native IP access to native management features on connected devices is available only after the authorized user has establish a trusted connection. VPN tunnels are required for a user to obtain native IP access either by going through the Web Manager or by entering ssh with the nativeipon device management command.

CAUTION: As discussed in the user's guide, unlike Native IP access, DirectCommand access automatically establishes the needed trusted connection. Also, for Native IP to work properly, the authentication method configured for the SP manager must be the same as the authentication method assigned to the target device.

Once a user has been authenticated and the user's authorization to access a target device has been checked, a user with a VPN connection has unlimited access to the target device. The SP manager cannot control whether a connected target device allows unrestricted access to the rest of the network; therefore, administrators must take care when configuring users of the target devices to protect the security of the network.

VPN connections establish encrypted communications between the SP manager and the user's workstation. The encryption creates a security tunnel for communications through an intermediate network which is untrustworthy. The user's workstation and the SP manager take care of encryption and decryption on their end.

An administrator must make sure that the appropriate service for the desired type of VPN connection is enabled (either PPTP or IPSec) on the MergePoint 5224/5240 SP manager before configuring a VPN connection profile on the SP manager for the type of VPN connections to be used.

The SP manager listens for the connection attempt from the IP addresses specified in its connection profiles and grants or denies the access.

Table 4.8 lists the VPN client system requirements and limitations.

Table 4.8: VPN Client System Requirements and Limitations

Platform	PPTP	IPSec
Windows	• Windows XP • Windows 2000 • Windows NT • Windows ME • Windows 98 • Windows 95 with DUN1.3 update Supported authentication method: MS-CHAPv2 **NOTE:** Only local or RADIUS authentication types can be used because the MS-CHAPv2 protocol does not work with other authentication types, such as LDAP, Kerberos or TACACS+	• Windows XP • Windows 2000 IPSec must be running on the workstation being used to manage target devices through the SP manager. Supported authentication types: • X.509 certificates (which require the administrator to manually create the certificate files in /etc) • Preshared key (PSK) requires a static IP • ESP and AH authentication protocols (also called encapsulation methods) • RSA Public Keys and Shared Secret **NOTE:** If the RSA public key authentication method is chosen, the generated keys are different on each end. When shared secret is used, the secret is shared on both ends.
Linux	PPTP client (pptp-linux)	OpenSWAN
MacOS X	Internet Connect application	MacOS X 10.2 or later

The user must perform the tasks in the following list to configure a VPN tunnel:

- Obtain from the administrator the values used in creating the VPN connection profile on the SP manager end including the PPTP username and password if PPTP is being used.
- Configure a VPN connection profile on the user's remote computer.
- If a route is needed to enable the user's workstation and the SP manager to exchange packets, specify it in the IPSec connection profile or create a route manually.
- Before attempting to access the native IP feature on the SP manager, the user must create the VPN tunnel from the user's computer.

IPSec VPN connections

The values needed for configuring IPSec VPN connections are shown in the following table.

Table 4.9: IPSec VPN Configuration Information for Administrators and Users

Value Name	Description
Connection name	Any descriptive name you choose.

Table 4.9: IPSec VPN Configuration Information for Administrators and Users (Continued)

Value Name	Description
Authentication protocol	• AH • ESP
Authentication method	• RSA public keys • Shared secret
Boot action	• Ignore • Add • Start • Add and route
Remote (Right)	
ID	@workstation_name
IP address	IP address of the user's workstation.
Next hop	Leave blank if the user's workstation and the SP manager are able to exchange packets. If a route must be set up to enable communications, enter the IP address of a host or network, so the IPSec can use the IP address to set up the needed route. Requires the Add and route boot option to also be selected.
Subnet	Leave blank.
Preshared key	Required if shared secret is selected as the authentication method.
RSA key	Required if RSA public keys is selected as the authentication method. The generated key for the remote computer, which the administrator must obtain from the user.
Local (Left)	
ID	@<SP manager_name>
IP address	Public IP address of the SP manager.
Next hop	Leave blank if the user's workstation and the SP manager are able to exchange packets. If a route must be set up to enable communications, enter the IP address of a host or network, so the IPSec can use the IP address to set up the needed route. Requires the add and route boot option to also be selected.
Subnet	Network IP address and netmask for the private subnet where the target devices reside that are going to be accessed through the SP manager.
Preshared key	Required if shared secret is selected as the authentication method.
RSA key	Required if RSA public keys is selected as the authentication method. The administrator generates an RSA key for the SP manager.

The administrator must perform the following tasks on the MergePoint 5224/5240 SP manager:

- Make sure that the IPSec service is enabled.
- Configure an IPSec VPN connection profile.
- Give the user the parameters used to configure the IPSec connection profile. One way to do this is to email the user a copy of the relevant portions of SP manager's ipsec.conf file.

The authorized user must perform the following tasks:

- Use the same values used by the SP manager administrator to create an IPSec VPN connection profile on the user's workstation.

  If the administrator emails the relevant portions of the ipsec.conf file from the SP manager, use it to replace the same section in the workstation's ipsec.conf file.
- Ensure that routes are in place to allow IPSec communication with the SP manager and also to allow packets to the target device to be routed through that tunnel.
- Create the IPSec VPN connection.

NOTE: If a virtual network has not been configured, the user may need to create a separate tunnel to each private subnet they wish to access. If a virtual network has been configured, the user needs only to create a single tunnel to the virtual network.

- Use either a browser or ssh on the command line to access the SP manager, using the appliance-side IP address. Use the appliance-side IP address configured when the private subnet or virtual network to which the tunnel is connected was being configured.
- Through the SP manager, enable native IP access to the target device.

PPTP VPN connections

For an authorized user to access native IP functionality on a connected SP, the user must create a VPN connection to the SP manager. An authorized user can create PPTP VPN connections from Linux, Windows or Macintosh operating systems.

The tasks listed below must be performed by the SP manager administrator before any user can make a PPTP VPN connection:

- Create a VPN connection profile on the SP manager specifying a pool of addresses for the SP manager and for the remote user's computer at the other end.

  When the user creates the PPTP VPN connection, PPTP creates a new virtual interface on the user's host and assigns an IP address from the SP manager's IP address pool to the interface. The user must use this address when connecting to the SP manager to enable native IP access to a target device.
- Authorize the user for PPTP access and provide the user with the PPTP password, which may be different from the user's password for accessing the SP manager.
- Authorize the user for native IP access to one or more target devices.

The user must perform the following tasks to enable PPTP on the user's workstation:

Make sure the workstation can access the SP manager by entering the SP manager's public IP address in a browser to try to bring up the Web Manager.

- If a network or host route is needed, create a route to the private subnet where the target device resides or to the real or virtual IP address of the target device.
- Make sure a PPTP client is running on the user's workstation.
- Configure a PPTP VPN connection profile with the following information obtained from the SP manager administrator:
  - PPTP server address = SP manager public IP address (203.1.2.3)
  - Username = SP manager username
  - Password = PPTP password
- Make the PPTP VPN connection.
- Enter the ifconfig or ipconfig command on the command line of the user's workstation to discover the IP address assigned to the SP manager's end of the PPTP link.
- Enter the SP manager's PPTP-assigned address either in a browser or with ssh on the command line to access the SP manager.
- Create a static route to inform the workstation that the target devices to be contacted are at the other end of the point-to-point link at the SP manager's PPTP-assigned address.
- If multiple private subnets have been configured without a virtual network (DNAT), then create a route for each subnet.
- Access the target device and enable native IP access.

CAUTION: Remind users to always disable native IP before closing the PPTP VPN connection to prevent other users from potentially being able to obtain unauthorized and unauthenticated access to native IP features of the target device.

Table 4.10 describes the values for configuring a PPTP profile.

Table 4.10: Fields for Configuring a PPTP Profile

Field	Purpose
PPTP local address pool	Assign an IP address or range of addresses to be used whenever a user creates a PPTP VPN connection to the SP manager.
PPTP remote address pool	Assign a remote IP address or range of addresses to be used whenever a user creates a PPTP VPN connection to the SP manager. Specify a pool of addresses in the form 10.0.0.100-110.

See *VPN on the MergePoint 5224/5240 SP Manager* on page 33 for more information.

DirectCommand on the MergePoint 5224/5240 SP Manager

As described in the MergePoint 5224/5240 Service Processor Manager User Guide, DirectCommand allows authorized users to access native management features on connected SPs without requiring a VPN tunnel to be created. An administrator can assign the DirectCommand authorization to users through the Web Manager, the cli utility or DSView 3 software.

In the Web Manager, the same permission (Native IP and DirectCommand) is used to grant DirectCommand access and to grant Native IP access. In the cli, setting either the nativeip or directcommand parameter to yes for a device grants the user both Native IP and DirectCommand access to the device.

CAUTION: For DirectCommand to work properly, the authentication method configured for the SP manager must be the same as the authentication method assigned to the target device authentication setting.

Message Logging (With Syslog) on the MergePoint 5224/5240 SP Manager

The administrator can set up logging of messages about the following types of events:

- Events of interest from the SP manager
- Events of interest obtained by filtering data during device console connections with connected devices
- Overcurrent status from a connected MergePoint PM IPDU
- Sensor alarms generated by sensors on target devices

Messages can be sent to central logging servers, called syslog servers. Messages can also be sent to the console or to the root user or both.

Message filtering levels

Messages can be filtered according to their severity, based on any or all of the levels that the administrator can select from the following list.

- 0 - EMERG (Emergency)
- 1 - ALERT
- 2 - CRIT (Critical)
- 3 - ERROR
- 4 - WARNING
- 5 - NOTICE
- 6 - INFO
- 7 - DEBUG

Syslog servers

Syslog servers run on operating systems that support system logging services, usually UNIX-based servers with the syslogd configured.

Tasks for configuring syslog messages

See Chapter 4 for the tasks related to configuring syslog messages and destinations through the Web Manager. See Chapter 7 for how to use cli to configure syslogging.

Ethernet Ports on the MergePoint 5224/5240 SP Manager

The SP manager's two public Ethernet ports are used for connecting to the public (or management) network. The managed private side of the SP manager is isolated from the public side to ensure security. Access to all connected servers is consolidated through the one publicly known IP address.

Private Ethernet ports

The SP manager is aware of only a single interface to the private network priv0 for communicating with the target devices. priv0 sends packets to and receives packets from the private Ethernet ports.

Each private Ethernet port may be connected to one or to multiple SPs. For example an Ethernet port may be connected to a blade manager with multiple SPs, and in those cases a single private Ethernet port may require multiple IP addresses.

All communication among private Ethernet ports is blocked unless priv0 is the sending or receiving port.

Public Ethernet ports

On the public side of the SP manager, the primary and secondary Ethernet ports are referred to as eth0 and eth1. Optionally added Ethernet PC cards are referred to as eth2 and eth3, and if they are present, they are treated as public interfaces.

Failover

The secondary Ethernet port on the SP manager can optionally be configured for failover, which is also referred to as bonding. Failover is important for high-availability environments where constant accessibility is required to support mission-critical applications. Failover automatically redirects traffic from the primary Ethernet port to the secondary Ethernet port if the primary interface fails. The primary Ethernet port continues to be monitored, and when it starts functioning again, traffic is then automatically redirected back through the primary Ethernet port again. All connection sessions continue without interruption.

With failover, both the primary and secondary Ethernet ports are assigned a single IP and single MAC [Ethernet] address.

After failover is enabled, the bonded Ethernet interfaces are referred to as bond0.

For example, when failover is set, the ifconfig command lists bond0 along with eth0 and eth1 as shown in the following screen example. Note that the HWaddress [MAC address] and inet addr [IP address] are identical for bond0, eth0 and eth1.

```
[root@ONB /]# ifconfig
bond0Link encap:Ethernet  HWaddr 00:60:2E:00:4F:97
inet addr:172.20.0.131  Bcast:172.20.255.255  Mask:255.255.0.0
eth0Link encap:Ethernet HWaddr 00:60:2E:00:4F:97
inet addr:172.20.0.131 Bcast:172.20.255.255  Mask:255.255.0.0
...
eth1Link encap:Ethernet  HWaddr 00:60:2E:00:4F:97
inet addr:172.20.0.131  Bcast:172.20.255.255  Mask:255.255.0.0
```

Ethernet media configuration

Administrators may configure a specific speed for the public Ethernet interfaces. The default is Auto Negotiation.

For more information, see the following sections:

- *Configuring Network Interfaces in the Wizard* on page 62
- *To configure the network interfaces (Wizard):* on page 63

Table 4.11 shows the values to use when configuring network interfaces.

Table 4.11: Network Interfaces Configuration Values

Settings	Notes
Host name	Default: MergePoint<model_number>, for example MergePoint5224
Domain name	Domain name used on the domain name server (DNS)
Primary DNS server	IP address for a primary DNS server on the same subnet as the SP manager
Secondary DNS server	IP address for an optional secondary DNS server on the same subnet as the SP manager
Failover	Selecting *enabled* from the pull-down menu configures failover from the primary to the secondary Ethernet port if the primary port goes down

Table 4.12 shows the values to use when configuring Ethernet ports.

Table 4.12: Ethernet Port Settings

Settings	Notes
DHCP	DHCP is enabled by default on the SP manager's interfaces. If DHCP is enabled, the SP manager looks for a DHCP server on the same network. If a DHCP server cannot be located, the SP manager falls back to using the default IP address described below. The additional fields in the table rows below appear only if DHCP is not checked, because they are needed only when configuring a static IP address for the interface.
IP address	192.168.160.10 is assigned by default to eth0. If DHCP is not used, the SP manager IP address should be changed to an IP address with a network portion that is within the local network address range.
Network mask	The desired netmask in the form: 255.255.255.0.
Gateway IP	IP address for a gateway on the same subnet as the SP manager. The gateway IP is used to create a default route for the interface. If a host or network route is required, the administrative user should select Network - Static routes to configure the route.
MTU	The maximum transmission unit value for the Ethernet port. Default=1500.
Broadcast IP	The reserved broadcast IP address.

Dial-in and Callback Access

The administrator can configure dial-in or callback access to the SP manager using PPP through either an external modem connected to the modem port or to a PC modem, GSM or CDMA card. PC modem and phone cards can also be accessed for logins without PPP from a terminal emulation program. Administrators can use the Web Manager for configuration as described in *To configure the AUX port for IPDU power management:* on page 70. Administrators can also configure modems with the cli utility. See *Configuring Dial-ins Using cli* on page 122 for examples.

Table 4.13 shows the configuration options that apply whether a modem or phone card is being configured through the Web Manager or the cli utility.

Table 4.13: Modem and Phone Card Field and Menu Options

Field or Menu Option/cli parameter	Options/cli parameter	Notes
Access Type/type	• Autodetect/autoppp • Login/login • PPP/ppp • OTP/otplogin	• Autodetection means that either type of access (PPP or Login) may be automatically detected. When autodetect is selected in the Web Manager, all the fields for configuring PPP and Login appear on the same screen and must be filled out. When autoppp is set using cli as the modem access type, then the PPP options should be configured. • OTP/otplogin supports OTP authentication for only login access only to modem or GSM or CDMA PC cards.
Baud Rate/speed	300 to 460800	Default = 9600
Flow Control/data-flow	Flow Control/data-flow	Default = none
Modem Initialization/initchat	A modem initialization string (or chat string) of AT commands used to configure the modem or phone when it is turned on or when the communications software dials out to another modem or phone.	Example: initchat ATZ OK A longer example: TIMEOUT 10 \d\l\dATZ OK\r\n-ATZ-OK\r\n TIMEOUT 10 ATM0 OK\r\n TIMEOUT 3600 RING STATUS Incoming%p:I.HANDSHAKE ATA TIMEOUT 60 CONNECT @ STATUS Connected%p:I.HANDSHAKE
Callback/ cbphone_enable, cbphone	If callback is selected, a callback number must be entered.	

Power Management Options

Authorized users and administrators can power down, power up and reboot devices using either IPDU or SP power management after administrators perform the needed configuration using either the Web Manager or the cli utility.

- IPDU power management requires that one or more IPDUs are connected to the AUX port and that an administrator has configured the AUX port and authorized users for IPDU power management.
- SP power management requires that users are configured for access to the SP and authorized to perform SP power management actions.

Adding Options to the User's Console Login Menu

Regular users are configured with /usr/bin/rmenush as their default login shell. All users with rmenush as their login shell see the same menu whenever they log into the console. The administrator can configure the rmenush menu to display other options including links to additional submenus or commands by modifying the /etc/menu.ini file. See *Configuring the Users' Console Login Menu* on page 126 for more information.

Routing on the MergePoint 5224/5240 SP Manager

The administrator can configure routing for default, host or network routes using either the Web Manager or the cli utility.

Configuring the network interfaces in either of the two following ways sets up a default route for the interface.

- When DHCP is enabled for a network interface, the DHCP server assigns a default route to the interface.
- When DHCP is not enabled, if the administrator configures a gateway IP address, that IP address is used to create a default route.

If a host route or network route is required, the route is configured as a static route that applies to the primary interface.

MergePoint 5224/5240 SP Manager Notifications

The SP manager firmware includes syslog-ng, which can be configured through either the Web Manager or the cli utility to filter log messages sent by system daemons (such as messages from the cron daemon, crond) and by target devices. By default, the /etc/syslog/syslog-ng.conf file monitors messages from the following two files:

- /dev/log
- /proc/kmsg

Notifications can be configured to be sent to an administrator by one of the following methods:

- SNMP trap
- Pager
- Email

syslog-ng allows administrators to set up additional alarm triggers to filter messages based on the messages' facility, level or contents.

Alarm triggers must be specified in the following format:

```
function('one_or_more_criteria_connected_by_operators');
```

Supported operators are and, or and not.

The following line shows the syntax for a match function.

```
match('regular_expression_matching_a_text_string');
```

The following lines show example match functions.

```
match('regular_expression") and not match("regular_ expression');
match('[Ll]ogin") and not match("francisco');
```

See the filter functions section of the syslog-ng v1.6 reference manual at http://www.balabit.com/products/syslog-ng/reference-1.6/syslog-ng.html/index.html#filterfunc for more information.

See the following sections for how administrative users can configure notifications, alarms and email:

- *Configuring Notifications* on page 90
- *Configuring Sensor Alarms* on page 93
- *Configuring Outbound Email* on page 77

MergePoint 5224/5240 SP Manager Sensor Alarms

The SP manager may also be configured to periodically check sensor readings from SPs and to send alarms based on specified sensor values, using either the Web Manager or the cli utility. Alarms can be configured to be sent to administrators by one of the following methods:

- Syslog message
- SNMP trap
- Pager
- Email

The following table shows the fields for configuring sensor alarms.

Table 4.14: Values for Configuring Sensor Alarms

Values	Description
Device	Choose from a list of all target device.
Sensor	The literal string for the sensor (which can be obtained from the sensor logs from the target device), for example, Sys Fan 1.
Condition	• Trigger when value is >INSIDE< range. • Trigger when value is <OUTSIDE> range. • Trigger when value CHANGES.
Range	Applies to the INSIDE and OUTSIDE conditions. The low and high thresholds can be any numeric value, including floats. For example, for a fan whose average reading is 1470 RPR, you might want to specify a low threshold of 1000 and a high threshold of 1600.
Interval	A polling interval chosen by the administrator: a time in minutes or hours.
Action	• Syslog message trap. • Pager. • Email.
Comment	Any desired comment to identify the source of the alarm.

See *Configuring Sensor Alarms* on page 93 for how to configure sensor alarms through the Web Manager. See *sensoralarm* on page 161 for cli command instructions.

Target Device Configuration

When connecting devices to the SP manager, observe the following recommendations, as shown in Figure 4.1:

- Connect the dedicated Ethernet port on each device to one of the SP manager's private Ethernet ports.
- Connect the main Ethernet port(s) on target devices to a production network.
- Connect the SP manager's primary Ethernet port (eth0) to a local management network and usually to the Internet.

CAUTION: If a device has a single Ethernet port, that port would need to be attached to the production network, and the SP manager would need to be configured to communicate with the device over the production network. With this type of configuration, the SP manager would be unable to provide the same level of secure access to devices that it provides when it is configured as recommended.

Figure 4.1 illustrates connecting two servers that have SPs, with the SPs indicated by gray boxes. The same recommendations apply to connecting devices that do not have SPs but that have dedicated Ethernet ports that provide access to the devices' consoles.

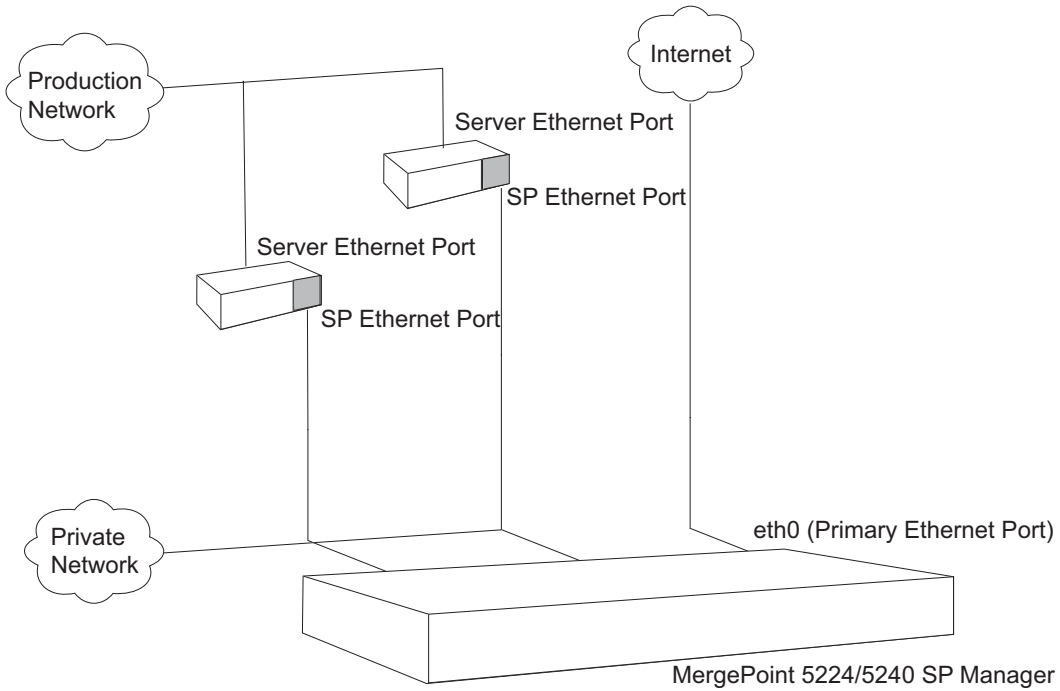

Figure 4.1: Recommended Target Device Configuration

Preparing an addressing scheme

Before configuring any target devices, the administrator must plan and implement an IP addressing scheme that reflects the needs of the organization.

As illustrated in Figure 4.1, the dedicated Ethernet ports on SPs and on other supported types of devices are connected to the private Ethernet ports. Each target device's dedicated Ethernet port needs an internal IP address assigned on the SP manager and configured for the interface. By implementing an addressing scheme, the administrator creates a pool of internal addresses that can be assigned to the devices' dedicated Ethernet ports and configured for the target device on the SP manager side.

While implementing the addressing scheme, the administrator assigns to the SP manager one or more private IP addresses in addition to the SP manager's public IP address. The SP manager's private IP address or addresses, which are referred to in the user interface as appliance-side addresses) are used by the following:

- Target Devices when talking to the private Ethernet ports of the SP manager
- Users who make PPTP or IPSec VPN connections to enable native IP access

Figure 4.2 shows some example IP addresses assigned.

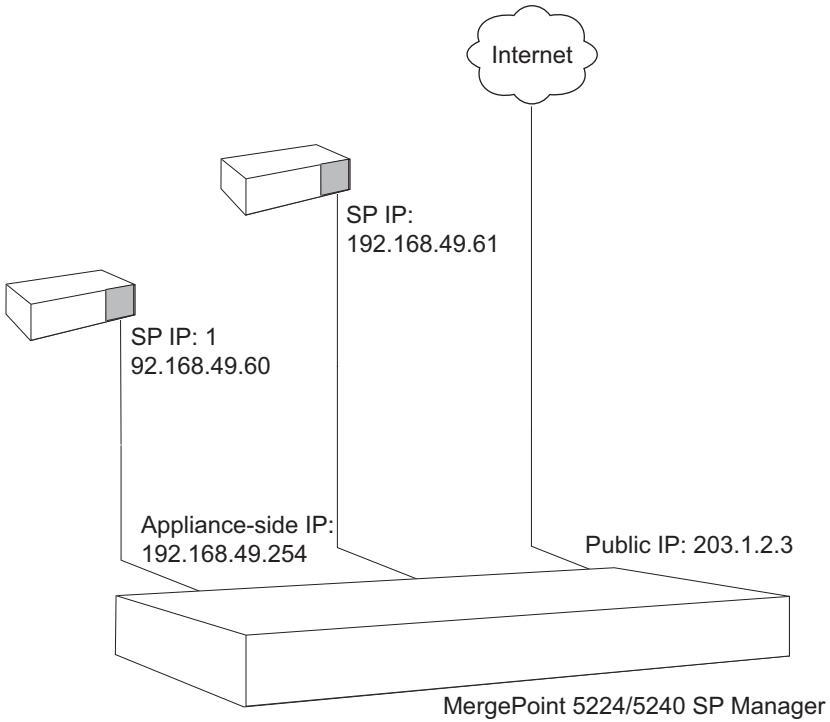

Figure 4.2: IP Addressing Example

See *Address configuration for target devices* on page 180 for the details needed for planning and implementing IP addresses.

Parameters for configuring target devices

The administrator configures connected target devices by assigning parameters described in the following table. Where more information is needed, the table provides links to where the parameters are described in more detail.

Table 4.15: Target Device Configuration Parameters

Parameter	Description
Name	Also referred to as an alias. A meaningful string that helps identify the target device and possibly its location, such as rack1_dev1_ibm306_rsa for an IBM 306 in the bottom row of rack 1. The assigned name can be used to access the target device by entering the name with the ssh command on the command line. See the MergePoint 5224/5240 Service Processor Manager User Guide for the syntax for using ssh with a target device's name to perform management functions on the server or other device.

Table 4.15: Target Device Configuration Parameters (Continued)

Parameter	Description
Login name and password	Obtained from the server's or device's administrator. Can be different from the username and password pair that the user enters to access the SP manager.
Target device group	If an administrator has configured one or more target device groups, the target device can be assigned to a target device group.
Type	The type of service-processor-management protocol or type of access. The following lists each of the defined SP and device types. • no type • ilo • rsa_II • drac • ipmi_1.5 • iipmi_2.0 • alom • devconsole • directcommand_only See *Address configuration for target devices* on page 180 for more information about assigning the correct device type.
Data buffering	Options for data buffering for the device are Yes, No or Default. Default accepts the global setting administratively specified for all target devices.
Private subnet	Used by the SP manager to communicate with target devices on the private network. See *Private Subnets and Virtual DNAT Networks on the MergePoint 5224/5240 SP Manager* on page 50 and *Why define private subnets?* on page 182 for more information about planning and implementing subnets and assigning them to target devices. Private subnets can be configured in the Web Manager on the Wizard Subnets screen or on the Network - Private Subnets screen as described in *Configuring Subnets and Virtual (DNAT) Networks in the Wizard* on page 63 and in *Configuring Private Subnets and Virtual Networks* on page 106.
Target device IP address	An IP address used by the SP manager to communicate with the target device. See *Preparing an addressing scheme* on page 46, *Address configuration for target devices* on page 180 and *Options for assigning IP addresses to target devices* on page 198 for more information about assigning IP addresses.
Virtual IP address (optional)	A virtual IP address to assign to the target device, which can be used to hide the real IP address from certain types of authorized users. Users who have native IP access, DirectCommand, SP console or device console access cannot be prevented from discovering the IP address of the dedicated Ethernet port that is connected to the SP manager. Virtual addresses are available only if a virtual network has been configured using DNAT. See *Why define virtual (DNAT) addresses?* on page 192 for more information about when virtual addresses are needed and how the administrator creates them.

Table 4.15: Target Device Configuration Parameters (Continued)

Parameter	Description
Description	A description that helps identify the target device, such as IBM xSeries 306 RSA II.
Authentication type	The authentication method to be used whenever a user accesses the target device. Can be different from the authentication method used for the SP manager, unless SSH tunneling is used to create a secure path for users who are authorized for native IP access. When an SSH tunnel is used, the SP manager and the target device must be using the same authorization method. See *MergePoint 5224/5240 SP Manager Authentication Options* on page 22. See also Table 4.1 on page 22 for a detailed list of authentication types supported for target devices.
Multisession	Configures whether or not multiple sessions are allowed for the target device when SoL access is used.

NOTE: If management commands do not work with a target device, the administrator may need to configure and assign a new target device type, by following the instructions under *Configuring target device types and command templates* on page 169.

Configuring new target device types

When adding a new target device, an administrator should follow the procedure under *To find out if an existing command template works with a new target device:* on page 178 to see if one of the default command templates works with the new target device. If not, an administrative user can use the Web Manager as described in *Configuring Target Device Types* on page 80 or the cli utility to either modify an existing device type or create a new device type.

Table 4.16: Values for Configuring Target Device Types

Parameters	Values	Notes
Protocol	• none • sh • telnet • ipmi	Protocol used for communications between the SP manager and target devices. Default = telnet.
Family	• iLO • RSA II • DRAC • IPMI 1.5 • IPMI 2.0 • ALOM • device console • custom 1 • custom 2 • custom3	Only assign one of the custom N families to a target device if a new Expect script has been created using one of the custom names (How administrators create new Expect scripts is described in Appendix C.)

Table 4.16: Values for Configuring Target Device Types (Continued)

Parameters	Values	Notes
Command template	• none • drac.default • rsa.default • ilo.default • rsa.limited.defaul • alom.default • ipmi_2.0.default, • devconsole.default	Target device of the following types do not need a command template: • IPMI-type devices (IPMI devices are managed using ipmitool commands). • Target devices being configured only for native IP access. • Target devices being configured for DirectCommand only access.
OEM Support (IPMI only)	• none • Supsermicro IPMI 1.5 • Intel SE7501WV2 IPMI 1.1 • Intel IPMI 2.0 with RMCP+ • IPMI 2.0 ICTS • IBM	Select among these options to adapt to a specific IPMI implementation in the list.
DirectCommand Options	Web Scheme: http or TCP Ports • https • Web port • Web path	Configure values to be used when DirectCommand is launched.
	TCP Ports • Port number • Description • Warning: No or Yes	Configure up to 20 TCP ports to set up port forwarding for DirectCommand.

Private Subnets and Virtual DNAT Networks on the MergePoint 5224/5240 SP Manager

Target devices should be isolated (as recommended under *Target Device Configuration* on page 45) on a management network that is separate from the production network and from the public network. To enable communications between the target devices and the SP manager, an administrator must configure at least one private subnet and may need to configure one or more optional virtual (DNAT) networks, based on a predefined addressing scheme. Deciding which addressing scheme to use is discussed in more detail with examples in *Target Device Configuration* on page 169.

Configuring private subnets

At least one subnet is needed to enable target devices that are connected to the SP manager's private Ethernet ports to communicate on the Internet via the SP manager's public IP address. Any number of private subnets may be configured.

After configuring a private subnet, the administrator then assigns to each target device the following two address-related parameters:

- The name of the private subnet
- An address within the private subnet's address range to be used by the target device when communicating with the SP manager

When a target device is not assigned a private subnet, the SP manager attempts to contact the target device using the default route and fails in the attempt, because devices are not connected on the public side of the SP manager.

Multiple private subnets may be needed if IP addresses are already assigned to connected target devices' Ethernet ports if the IP addresses are not in the same range.

Private subnets can be configured in the Web Manager on the Wizard Subnets screen or on the Network Private Subnets screen as described in *Configuring Subnets and Virtual (DNAT) Networks in the Wizard* on page 63 and *Configuring Private Subnets and Virtual Networks* on page 106. For more details about setting up subnets, see *Address configuration for target devices* on page 180.

Subnets are defined using the values described in Table 4.17.

Table 4.17: Fields on the Private Subnet Configuration Dialog

Field	Definition
Private subnet name	Any meaningful name chosen by the administrator.
Appliance side IP address	Address for the SP manager and target devices to use when communicating with each other. This address must be within the private subnet's IP address range.
Subnet mask	Used to define the range of addresses available on the subnet.

The SP manager derives the range of addresses in the subnet from the appliance side IP address and the subnet mask. The SP manager uses the specified information to create a route to the subnet in the SP manager's routing table.

Example

When the administrator defines an appliance-side IP address of 192.168.0.254 and a subnet netmask of 255.255.255.0, the private subnet address derived from this configuration is 192.168.0.0. Since the broadcast address is 192.168.0.255 (by convention**)** and the SP manager's address is 192.168.0.254, the administrator can assign any of the remaining available addresses between 192.168.0.1 and 192.168.0.253 when configuring target devices.

Configuring virtual networks (DNAT)

The administrator should define a virtual network based on Destination Network Address Translation (DNAT) in the following cases:

- When multiple non-contiguous private subnets must be supported by a single network route (or, in the case of IPSec, a single tunnel) on the client for VPN or native IP access. This would be the case when target devices are already configured using IP addresses from multiple address ranges and it is not feasible to change the previously defined IP addresses
- When it is important to hide the addresses of the connected target devices from users by the use of virtual IP addresses

Virtual networks are defined using the values described in Table 4.18.

Table 4.18: Values for Configuring Virtual Networks

Field	Description
Address	IP address to assign to the SP manager from the virtual network's address range. For example, if the virtual IP address of the network is 10.0.0.0, 10.0.0.254 would be a possible valid IP address for the SP manager.
Netmask	Netmask is used in combination with the network address portion of the Address above to define the address range of the virtual network.

Tasks for configuring IP addresses

The administrator may configure IP addresses using the Web Manager or the cli utility. See Appendix C for additional details about preparing an addressing scheme.

Data Buffering on the MergePoint 5224/5240 SP Manager

The appliance supports the buffering (storing) of data from the consoles of target devices so that the data can be monitored to detect events of interest and, when appropriate, generate alarms. Enabling data buffering can be done through the Web Manager or by using the cli utility. Configuring where data buffer files are stored must be done manually.

The administrator can configure a default for data buffering and then configure each target device to use the default or not. An administrator can configure data buffering either by using the Web Manager or by using the cli utility as described in the following sections:

- *Configuring Target Devices in the Wizard* on page 65 and *spmanager* on page 148
- *spmanager server* on page 162

By default, the buffered data is stored in RAM. The administrator may manually configure the storage of data either on a directory mounted from an NFS file server or on a PC Flash memory card. See *Configuring Storage of Buffered Data* on page 111.

Firewall/Packet Filtering on the MergePoint 5224/5240 SP Manager

Packet filtering on the SP manager is controlled by chains and rules that are configured in iptables. For more details about predefined chains and rules, see *Chains* on page 53 and *Rules* on page 54.

Both the Web Manager and the cli utility provide a way for the administrator to add rules and to edit or delete any added rules:

- Because the SP manager filters packets like a firewall, the Web Manager menu option under Network is titled Firewall.
- The cli utility provides the iptables command to perform the same tasks, because when rules are added, edited or deleted, the corresponding iptables are updated.

By default, the SP manager does not forward any traffic between private and public networks. The administrator might want to add rules to allow some limited communications between specific target devices on the private network and the public network.

CAUTION: It is possible for an administrator to create rules that circumvent the access controls on a target device.

Chains

A chain is a kind of named profile that includes one or more rules that define the following:

- A set of characteristics to look for in a packet
- What to do with any packet with all the defined characteristics

The SP manager comes with a number of built-in chains with hidden rules that are preconfigured to control communications between target devices that are connected to the private Ethernet ports and devices on the public side of the SP manager. The default chains are defined in filter and nat iptables. The mangle table is not used.

The built-in chains are named according to the type of packets they handle, as shown in the following lists. The first three chains are in the iptables filter table: INPUT, OUTPUT and FORWARD.

The three chains in the nat table are: PREROUTING, POSTROUTING and OUTPUT. These chains implement NAT (network address translation) including the redirecting of packets addressed to a virtual IP to the target device’s real IP address and the hiding of the target device’s real IP address when the target device sends packets to the authorized user.

Rules

Each chain can have one or more rules that define the following:

- The packet characteristics being filtered. The packet is checked for characteristics defined in the rule, for example, a specific IP header, input and output interfaces and protocol.
- What to do when the packet characteristics match the rule. The packet is handled according to the specified action (called a Rule Target, Target Action or Policy).

When a packet is filtered, its characteristics are compared against the rules one-by-one. All characteristics must match.

Add rule and edit rule options

When you add or edit a rule, you can define any of the options described in the following table.

Table 4.19: Filter Options for Packet Filtering Rules

Filter Options	Description
Protocol	You can select a protocol for filtering from one of the following options: • ALL • TCP • UDP • ICMP • GRE • ESP • AH
Source IP/mask Destination IP/mask	A host IP address or subnetwork IP address in the form: *hostIPaddress* or *networkIPaddress/NN*. If you specify a source IP, incoming packets are filtered for the specified IP address. If you specify a destination IP, outgoing packets are filtered for the specified IP address.
Input or Output Interface	The input or output interface used by the incoming or outgoing packet. Choices are: • Public 1 (eth0) • Public 2 (eth1) • Failover (bond0) • PCMCIA (eth2) • PCMCIA (eth3) • Any private port (priv0)
Fragments	The types of packets to be filtered: • All packets and fragments • Head fragments and unfragmented packets • Non-head fragments only
Rule target	• Accept • Drop • Reject

Any of the options in Table 4.19 can be given the inverted flag, so that the target action is performed on packets that do not match any of the specified criteria. For example, if only the two following criteria are specified - DROP is the target action, and Inverted is specified for a specific source IP address - any packets arriving from any other IP address will be dropped.

Tasks for administering packet filtering

Administrators can specify packet filtering by adding new rules for existing chains and editing or deleting administrator-added rules. See Chapter 4 for how to use the Web Manager to add or modify rules and Chapter 6 for how to use the cli iptables command to configure rules for built-in chains.

How Configuration Changes Are Handled

The following bulleted items give an overview of how the MergePoint 5224/5240 SP manager handles configuration file changes:

- When an administrator performs configuration tasks, changes are stored in RAM memory until the administrator takes a specific action to save the changes in configuration files.
- Unless changes are saved in configuration files, they do not persist after a reboot.
- The administrator can back up changed configuration files at any time.
- The SP manager maintains a backed up copy of the factory-default configuration files.
- The administrator can restore the factory default configuration files or restore any backed-up copies of the configuration files.
- The current state of the configuration files is maintained after a software upgrade. This allows you to upgrade software on the SP manager without losing all user and target device configurations. After software upgrade, the administrator can optionally perform the following tasks:
  - Return from the current state to the last backed-up copy of the configuration files.
  - Return to the factory default configuration files.
- When an administrator adds a new application, script or configuration file to the system, the root user must add the pathname to the file to the list of files to be backed up and restored.

CHAPTER 5

Using the Web Manager

Two types of administrative users can access all the Web Manager functions:

- An administrator who knows the password for the admin account, which is configured by default
- An optionally added administrative user (a regular user whose account is in the admin group)

Administrative users, like regular users, can access the Web Manager from a browser using HTTP or HTTPS either over the Internet or through a dial-in or callback PPP connection. Also like regular users, administrative users can use default menu options that appear on the first Web Manager screen after login to access devices, manage power and to change their own passwords.

In addition to being able to perform all the tasks regular authorized users can perform, administrative users can use the Web Manager for configuring users, devices and other MergePoint 5224/5240 SP manager features that enable the enforcement of the organization's security policies.

Only one administrative user can connect to the Web Manager at a time. A prompt appears if another administrative user is currently logged in with the option to either cancel the login attempt or to log out the currently logged-in administrative user.

NOTE: For security, a login session times out after a defined period of inactivity. An administrator can change the time-out value as described in *Changing Web Manager Time-outs* on page 131.

To log into the Web Manager as an administrative user:

This procedure assumes you know the password for the admin account or the username and password for an administrative user account and that you have either a network connection or a dial-in connection over a phone line.

1. Enter the IP address of the SP manager in a supported browser. The Web Manager login screen appears.
2. Enter the username and password.
3. Click the *Login* button.

NOTE: All procedures in this chapter assume you are logged into the Web Manager as an administrative user.

Features of Administrative Users' Screens

Callouts in the following figure indicate unique features of the Web Manager that appear only when an administrative user logs in.

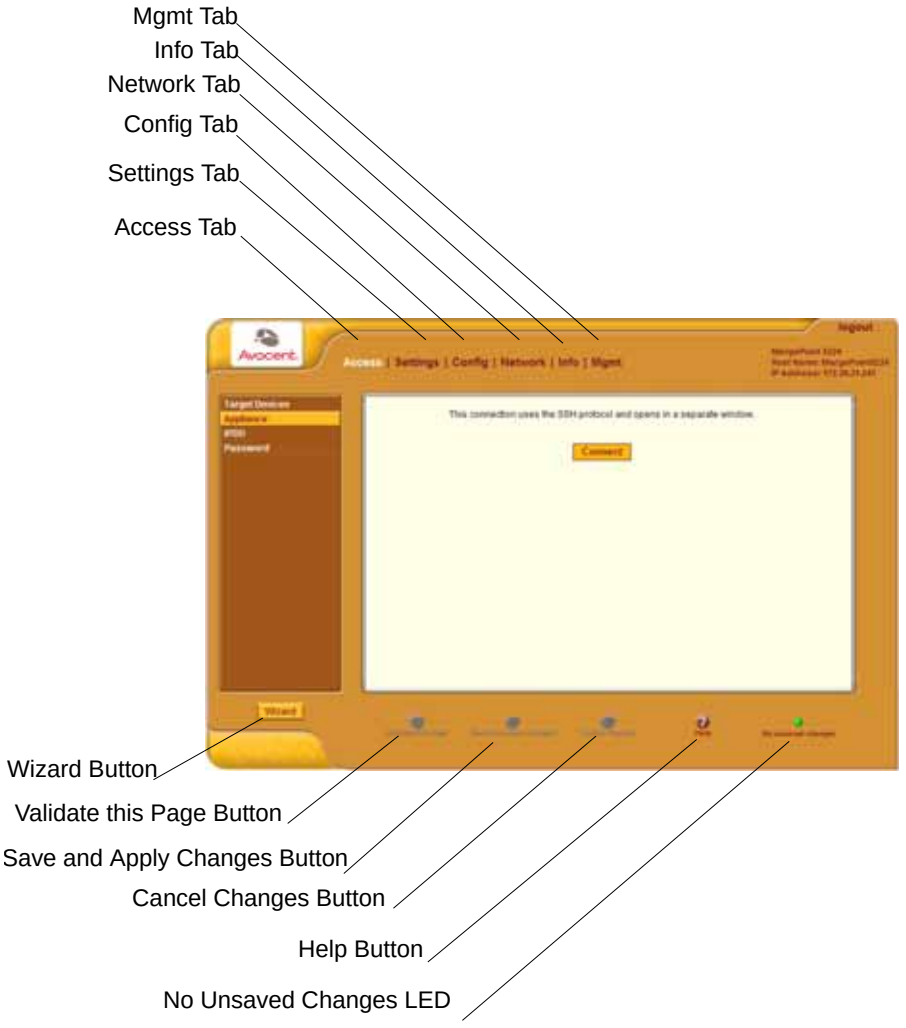

Figure 5.1: Administrative User Options on the Web Manager

Selecting a tab from the top menu changes the list of left menu options.

An option in the left menu (such as IPDU in Figure 5.1) often has several related screens associated with it. The related screens are accessed as tabs after the option is selected.

The *Wizard* button brings up the configuration wizard, as described in *Web Manager Wizard* on page 60.

The *Validate this Page* button allows the administrative user to try the configuration changes on a page without saving them.

The *Save and Apply Changes* button saves the changes into the configuration files.

The *Cancel Changes* button leaves the configuration files unchanged and the No Unsaved Changes LED stops blinking.

The No Unsaved Changes LED blinks from the time any changes are made until either the S*ave and Apply Changes* or *Cancel Changes* buttons are clicked.

For more about how administrators can save, back up and restore configuration files, see *How Configuration Changes Are Handled* on page 55.

Dialogs in the Web Manager

Dialogs are screens that appear when an administrative user clicks an *Add* or *Edit* button. While dialogs are active, the buttons at the bottom and the menu options are grayed out. The grayed out options and buttons become active again only after the administrative user clicks either the *OK* or *Cancel* button.

Figure 5.2: Example Dialog: Devices Configuration in Wizard Mode

Web Manager Wizard

Clicking the *Wizard* button brings up a window with a list of options in the left menu for performing basic configuration of the SP manager.

Figure 5.3: MergePoint 5224/5240 SP Manager Configuration Wizard Screen

After the *Next* button is clicked on the last screen of the Wizard, the screen shown in Figure 5.4 appears. Clicking the *Next* button again saves all changes made on any of the previous Wizard screens.

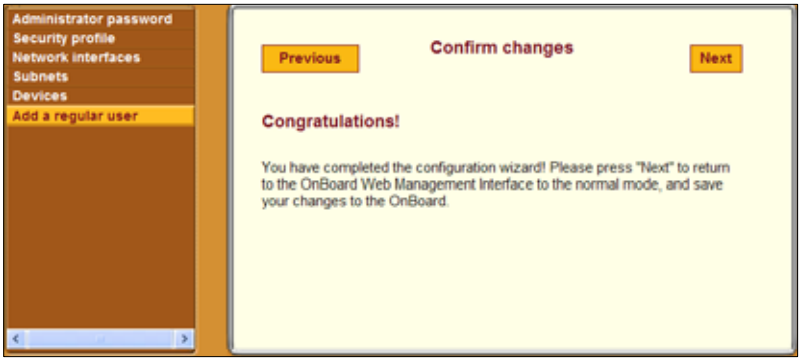
Administrator password
Security profile
Network interfaces
Subnets
Devices
Add a regular user
Previous
Confirm changes
Next
Congratulations!
You have completed the configuration wizard! Please press "Next" to return to the OnBoard Web Management Interface to the normal mode, and save your changes to the OnBoard.

Figure 5.4: Wizard Confirm Changes Screen

Changing the Administrative User's Password in the Wizard

The Administrator password option on the Wizard menu brings up a window for changing the password of the currently logged in administrative user.

CAUTION: If the default password cyclades is still in effect, changing the password now is essential to reduce the risk of intrusion. Leaving the password unchanged leaves a security breach that makes all connected equipment vulnerable.

To change the administrative user's password (Wizard):

1. Click the *Wizard* button. The Administrator password menu option is highlighted and the Changing <administrative_username> password screen is active by default.
2. Enter a new password for the administrative user in the Password field and retype it to verify.
3. Click *Set Password*.

Selecting a Security Profile in the Wizard

When the Security profile option is selected from the Wizard menu, the screen identifies the name of the security profile currently in effect. For more details about the services and features defined by default security profiles and about how customized profiles can be created, see *Security Profiles* on page 25.

NOTE: Putting another security profile into effect could disable or enable services that may have been turned on or off by some other means. For more details, see *Services* on page 27.

Clicking the Proceed button on the Security Profile Caution screen brings up the Configure the Security Profile dialog. An administrative user can use the dialog to select one of the default security profiles or configure a custom security profile.

The Moderate profile is the default option selected on the Security level menu.

If the administrative user chooses a preconfigured security profile or creates a custom profile and clicks *OK*, the red Unsaved changes button blinks, and the Security Profile screen reappears showing the newly selected security profile's name.

To select or configure a security profile (Wizard):

1. Click the *Wizard* button.
2. Select the *Security profile* option in the left menu bar.
3. Click the *Proceed* button.
4. Select a security profile from the Security Level pull-down menu.
5. If you select the *Custom* profile, make sure the checkboxes are checked next to services and features you want to be enabled and make sure the checkboxes are clear next to services and features you want to be disabled.

6. Click *OK*. The security profile confirmation screen appears.
7. Click *Save and apply changes*.
8. Click *Next*, if desired, to go to the next Wizard screen.

Configuring Network Interfaces in the Wizard

By selecting the Network interfaces option from the Wizard menu, the administrative user can configure network interfaces and Ethernet ports. See *Configuring failover* on page 62 and *Configuring primary and secondary Ethernet ports* on page 62 for more information. Table 4.11 on page 40 shows the values to use when configuring network interfaces.

Clicking the *Next* button on the Network Interfaces screen brings up one of two screens for configuring the Ethernet ports, depending on whether failover is enabled or disabled. Table 4.12 on page 41 shows the values to use when configuring Ethernet ports.

Configuring routes

Configuring the network interfaces in either of the two following ways sets up a default route for the SP manager:

- When the *DHCP* checkbox is checked on any of the network interface screens, the DHCP server assigns the SP manager a default route.
- If the *DHCP* checkbox is not checked, the gateway IP specified by the administrative user in the Gateway IP field is used to create a default route for the interface.

If a host or network route is required, the administrative user should select Network - Static routes to configure the route.

Configuring failover

If failover is enabled on the Network Interfaces screen, clicking the *Next* button brings up a screen for configuring the failover device. Clicking the *Next* button brings up the subnet configuration screen.

With failover enabled, the secondary Ethernet interface becomes bonded to the primary Ethernet interface, and the secondary Ethernet interface becomes active only if the primary Ethernet port is not available. As a result, the values entered in the fields on the failover configuration screen apply to the single bond0 interface.

Configuring primary and secondary Ethernet ports

If failover is disabled, the administrative user can configure each Ethernet port separately in the following ways:

- Enable or disable each Ethernet port
- Enable or disable DHCP
- If DHCP is disabled, configure each port for static IP addressing

To configure the network interfaces (Wizard):

1. Click the *Wizard* button.
2. Select the *Network interfaces* option in the left menu bar.
3. Modify the name in the Host name field, if desired.
4. Enter or modify an existing DNS domainname in the Domain name field.
5. Enter or modify the IP address for a primary DNS server into the Primary DNS field.
6. Enter or modify the IP address for a secondary DNS server in the Secondary DNS field.
7. Enable or disable failover by selecting the desired option from the Failover pull-down menu.
8. Click the *Next* button.
   - If failover is disabled, clicking the *Next* button brings up the first of two screens for configuring the primary and secondary Ethernet ports.

NOTE: Connecting the secondary Ethernet port to a separate network and assigning a separate IP address is optional, so you can skip the screen for configuring the secondary Ethernet port, if desired.

   - If failover is enabled, clicking the *Next* button brings up a screen for configuring the failover device.
9. If desired, enable DHCP on any of the network interface configuration screens, by clicking the *DHCP* checkbox.
10. If desired, configure the selected Ethernet port to use a static IP address by performing the following steps:
    a. Disable DHCP by making sure the *DHCP* checkbox is not checked.
    b. Enter or modify the IP address in the IP address field.
    c. Enter or modify the netmask in the Network mask field.
    d. Enter or modify the IP address for a network gateway in the Gateway IP field.
    e. Enter or modify the maximum transmission unit value for the Ethernet port in the MTU field.
    f. Enter or modify the broadcast IP address for the Ethernet port in the Broadcast IP field.
11. If failover is disabled and the current Ethernet port is the primary Ethernet port, click the *Next* button and perform step 10 again on the secondary Ethernet port configuration screen for the secondary Ethernet port, if desired.
12. Click *Save and apply changes*.
13. Click *Next*, if desired, to go to the next Wizard screen.

Configuring Subnets and Virtual (DNAT) Networks in the Wizard

After selecting the *Subnets* menu option, from the Wizard menu, the administrative user should configure at least one private subnet and one or more optional virtual (DNAT) networks based on a predefined addressing scheme. Deciding which addressing scheme to use is discussed in *Private*

Subnets and Virtual DNAT Networks on the MergePoint 5224/5240 SP Manager on page 50 and in more detail in *Target Device Configuration* on page 169.

At least one subnet is needed to enable devices that are connected to the SP manager's private Ethernet ports to communicate on the Internet via the SP manager's public IP address. Any number of private subnets may be configured. Configuration of one or more virtual networks is optional.

Subnets are defined using the values described in Table 4.17 on page 51.

Virtual networks are defined using the values described in Table 4.18 on page 52.

CAUTION: Changing or deleting an existing private subnet changes the configuration of any device that was previously configured to use that private subnet; the private subnet is removed from the device's configuration, and on subsequent attempts to contact the device, the SP manager tries to use the default route. If changing or deleting a private subnet, make sure to reassign all affected devices to another private subnet to avoid making devices unavailable.

To add a private subnet (Wizard):

1. Click the *Wizard* button.
2. Select the *Subnets* option in the left menu bar.
3. Click the *Add Subnet* button.
4. Enter a meaningful name for the private subnet in the Private subnet name field.
5. Enter an IP address within the private subnet's network address range in the Appliance side IP address field.
6. Enter a netmask for the subnet in the Subnet netmask field.
7. Click *OK*.
8. Click *Save and apply changes*.
9. Click the *Next* button, if desired, to go to the next Wizard step.

To edit a private subnet (Wizard):

1. Click the *Wizard* button.
2. Select the *Subnets* option in the left menu bar.
3. Click the *Edit* button for the entry for the private subnet you want to change.
4. Accept or change the name of the private subnet in the Private subnet name field.
5. Accept or change the IP address in the Appliance side IP address field.
6. Accept or change the netmask for the subnet in the Subnet netmask field.
7. Click *OK*.
8. Click *Save and apply changes*.
9. Click *Next*, if desired, to go to the next Wizard screen.

To configure a private subnet and optional virtual network (Wizard):

1. Click the *Wizard* button.
2. Select the *Subnets* left menu option.
3. Under Virtual Network (DNAT) configuration, enter the IP address within the virtual network's network address range in the Address field.
4. Enter a netmask in the Netmask field.
5. Click *Save and apply changes*.
6. Click *Next*, if desired, to go to the next Wizard screen.

Configuring Target Devices in the Wizard

By selecting the Target devices option from the Wizard menu, the administrative user can configure individual target devices connected to the private Ethernet ports and can configure data buffering for all target devices. Target devices are defined using the values described in Table 4.15 on page 47.

CAUTION: All target devices connected to the private Ethernet ports must have a previously configured private subnet name assigned. Otherwise, the target device can only be accessed if it is connected to the public interface of the SP manager, which is strongly discouraged.

Make sure the following are complete:

- A private subnet has been created.
- An administrator has followed the procedure under *To use the sptemplate utility to create a new template:* on page 178 to find out if a default command template works with the new device and to create a new command template if needed.
- You know the username and password pair that are used for logging into the SP or device.

To configure data buffering for all target devices (Wizard):

1. Click the *Wizard* button.
2. Select the *Target devices* option in the left menu bar.
3. Select *Yes* or *No* from the Data buffering Default pull-down menu.
4. Click *OK*.
5. Click *Save and apply changes*.

To add a target device (Wizard):

1. Click the *Wizard* button.
2. Select the *Target device* option in the left menu bar.
3. Click the *Add new target device* button.
4. Enter a descriptive name for service processor or other type of target device in the Name field.

5. Enter the username and password pair used for logging into the device in the Login and Password fields and retype the password to verify.
6. If target device groups have been configured, select the device group from the Target device group pull-down menu.

NOTE: For how to add a target device group, see *To configure device groups:* on page 83.

7. Select the target device type from the Type pull-down menu.
8. Select a data buffering option, *Yes*, *No* or *Default* from the Data buffering pull-down menu.
9. Select a private subnet name from the Private subnet pull-down menu.

NOTE: For how to configure private subnets, see *To configure a private subnet:* on page 106.

10. Enter the real IP address for the device in the Target device IP address field.
11. If a virtual network has been configured as described in *Configuring virtual networks (DNAT)* on page 52, enter a virtual IP address for the device in the Virtual IP address field.
12. Enter a description in the Description field.
13. Select an authentication type from the Authentication type pull-down menu.
14. Select *Yes* or *No* from the Multisession pull-down menu.
15. Click *OK*.
16. Click *Save and apply changes*.

Configuring Regular Users in the Wizard

By selecting the *Add a regular user option* from the Wizard menu, the administrative user can configure user accounts. Users are defined using the values described in Table 4.2 on page 25.

CAUTION: Configuring device management actions for a user gives the user the same device management permissions for all configured devices. To configure a user with more or fewer device management permissions on one device than on another, the administrative user can use the Config - Users and Groups Screen.

To create and authorize a user for device management (Wizard):

1. Click the *Wizard* button.
2. Click the *Add a regular user* left menu option.
3. Enter a name in the Username field.
4. Enter identifying (GECOS-type) information in the Full name field.
5. Enter a password in the Password field and retype the password to verify.
6. To authorize the user for device management actions on all configured devices, check or leave unchecked the checkboxes next to the name of every allowed action.
7. Select one of the options from the PPP/PPTP access menu.

8. If you selected any PPP/PPTP option other than None, perform the following steps:
   a. Enter a password in the PPP/PPTP password field.
   b. Retype the password in the Retype password field.
9. Click *Save and apply changes*.
10. Click *Next* to go to the Confirm Changes screen.
11. Click *Next* to save all changes made in the Wizard and to return to the Web Manager.

Web Manager Access Menu Options for Administrative Users

The *Access* menu options available to administrative users are the same options available to regular users, except that administrative users can perform additional configuration on some of the screens.

Accessing the MergePoint 5224/5240 SP Manager Console through the Web Manager

After an administrative user clicks the *Access - Appliance* menu option and enters the correct password and is authenticated, then the administrative user can perform any of the following:

- Access the cli utility to perform command line configuration
- Run the spshell utility to access devices
- Enter commands that do not require root to succeed
- Run commands that require root to succeed by entering the sudo command followed by the name of the command

To access the console:

1. Select the *Access - Appliance* menu option.
2. If this is not the first time you accessed the console, the login prompt for the SP manager appears. Go to step 4.
3. If this is the first time you are accessing the SP manager's console, perform the following steps:
   a. Press **Enter** at the prompt to confirm the saving of the SP manager's IP address. A dialog box asks if you want to add the SP manager to your set of known hosts.
   b. Click *Yes*. The login prompt for the SP manager appears.
4. Log into the SP manager.
5. As desired, perform any of the following actions:
   - Run the **cli** utility to perform command line configuration.
   - Run the **spshell** utility to access devices.
   - Run other commands that do not require root to succeed.

Upgrading IPDU Software

Upgrading IPDU software is a two-stage process requiring the following two actions:

- An updated version of the IPDU software must be downloaded to the SP manager's /tmp directory.
- The administrative user must select the *Software Upgrade* tab under the Access - IPDU menu option and configure the upgrade.

On the IPDU Software Upgrade Screen, a directly connected IPDU is referred to as the Master Unit and any daisy-chained IPDUs are referred to as Slave 1 through Slave N.

NOTE: Daisy-chaining only works if all daisy-chained IPDUs are running the same version of the PM IPDU software. The administrator must ensure that all connected Cyclades PM IPDUs have the most recent version of the IPDU PM software.

To download Cyclades PM IPDU firmware:

1. Log into the console as an administrative user.
2. Change to the /tmp directory where the software must be downloaded.

   ```
   [admin@MergePoint5224 admin]# cd /tmp
   ```

3. Enter the **ftp** command to access ftp.cyclades.com.

   ```
   [admin@MergePoint5224 tmp]# ftp ftp.cyclades.com
   ```

4. Enter **anonymous** when prompted for the Name and press **Enter** when prompted for the password.

   ```
   Name (ftp.cyclades.com:admin): anonymous
   331 Please specify the password.
   Password: <Enter>
   ```

5. Change directories to /pub/cyclades/alterpath/pm/released and list the directories it contains.

   ```
   ftp> cd /pub/cyclades/alterpath/pm/released
   ftp> ls
   ...
   V_1.8.0
   V_1.9.0
   ```

   As shown in the previous screen example, the directories are named for the software release numbers. The latest version in the example is V_1.9.0. If the latest version at the ftp site is more recent than the version installed on the IPDU, continue with this procedure.

6. Change directories to the directory with the highest (latest) version number.

```
ftp> cd V_1.9.0
```

7. Use the **get** command to get the binary file (for example: PM_190.BIN) and enter pmfirmware as the destination filename.

```
ftp> get
(remote-file) PM_190.BIN
(local-file) pmfirmware
```

8. After the download completes, end the ftp connection and verify the presence of the pmfirmware file in the /tmp directory.

```
ftp> bye
[admin@MergePoint5224 tmp]
$ ls
...
pmfirmware
```

9. Log out from the console session and perform the next procedure to update the software.

To upgrade software on a connected IPDU:

1. Make sure that the most recent version of the Cyclades PM IPDU software has been downloaded and copied into the SP manager's /tmp directory with the filename pmfirmware.
2. Log into the Web Manager as an administrative user.
3. Select the *Access - IPDU - Software Upgrade* menu option. The Software Upgrade screen displays.
4. Click the *Refresh* button. If a /tmp/pmfirmware file exists containing a more recent version of the PM software than the one currently installed, the value next to Latest software version available changes to match the version in /tmp/pmfirmware, and an Upgrade button appears.
5. Click *Upgrade*. A dialog box displays while the software is being upgraded.
6. When the OK button displays on the dialog box, click *OK*.
7. Repeat step 5 and step 6 for all listed IPDUs until all are upgraded to the same level.

Configuring the AUX Port

The administrative user can use the Settings - AUX port screen to configure the AUX port when either of the two following types of optional devices is connected to that port:

- One or more PM IPDUs for IPDU power managment.
- An external modem for dial-in using PPP or login access. The values to select or to enter for modem configuration are described in Table 4.13 on page 42.

To configure the AUX port for IPDU power management:

This procedure assumes that a Cyclades PM IPDU is connected to the AUX port.

1. Select the *Settings - AUX Port* menu option.
2. Make sure the *Power Management* option is selected from the Profile menu.
3. (Optional) Enter a name for the connected IPDU in the Name field.
4. Click *Save and apply changes.*
5. Go to *Configuring IPDU Power Management* on page 70.

To configure an AUX port for modem access:

1. Select the *Settings - AUX Port* menu option.
2. Select *Modem* from the Profile menu.
3. Choose *Login, Autodetect, PPP* or *OTP* from the Modem access menu.
4. Select a baud rate from the Baud Rate pull-down menu.
5. If you chose either Login or Autodetect, select an option from the Flow Control menu.
6. Enter a modem chat string in the Modem Initialization field.
7. If you chose PPP or Autodetect, perform the following steps:
   a. Enter a local IP address or accept the default provided in the Local IP address field.
   b. Enter a remote IP address or accept the default provided in the Remote IP address field.
   c. Enable or disable authentication by checking or leaving unchecked the *Authenticating Required* checkbox.
   d. Accept or change the value in the MTU field.
   e. Accept or change the value in the MRU field.
   f. Accept or change PPP options as desired in the PPP Options field.
8. Enable callback, if desired, by performing the following steps.
   a. Check the *Use Callback* checkbox. The Callback Number field appears.
   b. Enter a callback phone number.
9. Click *Save and apply changes.*

Configuring IPDU Power Management

When an administrative user clicks the IPDU option under Settings, three tabs appear for configuring connected IPDU(s).

The first IPDU connected to the AUX port is called the Master Unit. An additional IPDU that is daisy-chained to the first IPDU is called a Slave Unit.

The IPDU power management configuration procedures assume that the user account has been defined as described under *To create and authorize a user for device management (Wizard):* on page 66.

Configuring Over Current Protection for an IPDU

When an administrative user selects the *Settings - IPDU - General* tab, a screen appears for setting overcurrent protection, so that if an overcurrent state occurs, an alarm notification is sent by means of a syslog message to the console or a buzzer or both. Cyclades PM IPDUs that are directly connected to the AUX port are called Master Units; daisy-chained IPDUs are called Slave Units. Each IPDU can have different settings.

When enabling overcurrent protection, the administrative user specifies a maximum number of amps entered either as a whole number or as a number with a decimal point (for example, 10 amps or 14.5 amps). When the maximum number of amps is exceeded, the SP manager generates an alarm:

- Checking *Enable syslog* causes syslog messages to be sent to the console
- Checking *Enable buzzer* causes a buzzer to sound on the IPDU

To enable overcurrent protection for an IPDU:

1. Select the *Settings - IPDU - General* menu option.
2. Check the *Enable Over Current Protection* checkbox, then perform the following steps:
   a. Click the *Edit* button next to the IPDU on which you want to set alarm threshold. The Edit Alarm Threshold for IPDU Dialog appears.
   b. Enter the appropriate number of amps for the selected type of IPDU in the Alarm Threshold field.
   c. Click *OK*. The IPDU - General screen appears.
3. To enable syslog messages to be sent to the console if the alarm threshold is exceeded, check the *Enable syslog* checkbox.
4. To cause a buzzer to sound on the PM if the alarm threshold is exceeded, check the *Enable buzzer* checkbox.
5. Click *OK*.
6. Click *Save and apply changes*.

Configuring Users to Manage Power Outlets on an IPDU

By selecting the *Settings - IPDU - Users* tab, an administrative user can authorize one or more regular users to manage power outlets.

Separate multiple usernames and sequential outlet numbers with commas, and indicate a range of outlet numbers with a hyphen (for example: user1,user2 and 1, 3, 5, 6-8).

To configure a user to manage power outlets on a connected IPDU:

1. Select the *Settings - IPDU - Users* menu option.
2. Click the *Add User* button.

3. Enter one or more comma-separated usernames in the Username field.
4. Enter one or more comma-separated outlets to manage in the Outlets field.
5. Click *OK*.
6. Click *Save and apply changes*.

Configuring Names and Power Up Intervals for IPDU Outlets

After selecting the Settings - IPDU - *Outlets* tab, an administrative user can assign a name to a power outlet and change power up interval (the number of seconds that must elapse between when the selected outlet is turned on and another outlet is turned on).

Specify intervals using whole numbers along or followed by decimals, such as 10 or 7.5. Clicking *OK* saves the entries.

To configure an alias and a power up interval for an IPDU outlet:

1. Select the *Settings - IPDU - Outlets* menu option.
2. To assign or change an outlet name, perform the following steps:
   a. Click the *Edit* button in the outlet's Name column. The outlet name dialog appears.
   b. Enter a name in the Outlet N name field.
   c. Click *OK*.
3. To assign or change an outlet's power-up interval, perform the following steps:
   a. Click the *Edit* button in the outlet's Interval column. The outlet power up interval dialog appears.
   b. Enter a number of seconds in the Outlet N power-up interval field.
   c. Click *OK*.
4. Click *Save and apply changes*.

Configuring PC Cards

By selecting the *Settings - PCMCIA* menu option, the administrative user can use the PCMCIA screen to insert, eject and configure PC cards. The following table shows how the three buttons on this screen are used.

The following procedure describes the configuration steps to begin configuring any PC card.

To begin configuring a PC card:

1. Select the *Settings - PCMCIA* menu option. The PCMCIA screen appears.
2. Click the *Insert* button on the line for the slot in which you are installing the PC card.
3. Insert the card into one of the slots on the front of the SP manager.
4. Click *OK*. The card type appears under the Card Type column.
5. Click the *Configure* button. The configuration dialog for the selected slot appears.

6. Select the desired the card type to configure from the pull-down menu.The card configuration dialog appears.
7. Perform the configuration for the type of card selected.

The following procedures assume that a PC card of the selected card type is inserted into a slot on the SP manager and that the steps under *To begin configuring a PC card:* are complete.

NOTE: Configuration of OTP authentication through the Web Manager is only supported for modem or GSM cards.

See Table 4.13 on page 42 for the values that an administrative user must select or to enter for modem configuration, if needed.

To configure a modem or GSM PC card:

1. Make sure that *Modem* or *GSM* are selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
2. Select either *Login*, *Autodetect*, *PPP* or *OTP* from the Modem Access Type pull-down menu.
3. Select an option from the Flow control pull-down menu.
4. Select a baud rate from the Baud rate pull-down menu.
5. Enter a modem chat string in the Modem Initialization field.
6. If you selected either the PPP or Autodetect modem access types, perform the following steps:
    a. Enter a local IP address or accept the default provided in the Local IP address field.
    b. Enter a remote IP address or accept the default provided in the Remote IP address field.
    c. Enable or disable authentication by checking or leaving unchecked the *Authenticating Required* checkbox.
    d. Accept or change the value in the MTU field.
    e. Accept or change the value in the MRU field.
    f. Enter PPP options as desired in the PPP Options field.
7. Enable callback, if desired, by performing the following steps.
    a. Check the Use Callback checkbox. The Phone Number field appears.
    b. Enter the remote user's modem or phone number to use when calling the user back.
8. Click *OK*.
9. Click *Save and apply changes*.

To configure an Ethernet PC card:

1. Make sure that *Ethernet* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
2. To enable DHCP, check the *DHCP* checkbox and go to step 4.

3. To define basic network parameters that enable the use of a static IP address, perform the following steps:
   a. Enter an IP address in the IP Address field.
   b. Enter a netmask in the Network Mask field.
   c. Enter the IP address for a gateway host or enter none in the Gateway field.
4. Click *OK*.
5. Click *Save and apply changes*.

To configure a wireless LAN PC card:

1. Make sure that *Wireless LAN* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
2. To enable DHCP, check the *DHCP* checkbox and go to step 4.
3. To define basic network parameters that enable the use of a static IP address, perform the following steps:
   a. Enter an IP address in the IP Address field.
   b. Enter a netmask in the Network Mask field.
   c. Enter the IP address for a gateway host or enter none in the Gateway field.
4. Enter a network name in the MyPrivateNet [ESSID] field.
5. Enter a channel in the Channel field.
6. Select either *Managed* or *Ad-hoc* from the Managed pull-down menu.
7. Click *OK*.
8. Click *Save and apply changes*.

To configure a compact Flash PC card:

1. Make sure that *Compact Flash* is selected from the Card Type pull-down menu on the PCMCIA card configuration dialog.
2. To mount a filesystem from the compact Flash memory, check the *Mount Compact Flash Card* checkbox.
3. Select an option from the File System menu.
4. Click *OK*.
5. Click *Save and apply changes*.

Configuring System Date and Time

By selecting the *Settings - Date/time* menu option, the administrative user can configure the timezone and how the SP manager sets its time and date.

To configure system date and time:

1. Select the *Settings - Date/time* menu option.

2. Select a timezone from the Timezone pull-down menu.
3. To enable the SP manager to get its time from an NTP server, perform the following steps:
   a. Select *Enable* from the Network Time Protocol pull-down menu.
   b. Enter the IP address of the NTP server in the NTP server IP field.
4. To manually define the date and time, perform the following steps:
   a. Enter the month, day and year in the Month, Day and Year fields.
   b. Enter the hour, minute and second in the Hour, Minute and Second fields.
   c. Click the *Refresh time* button.
5. Click *OK*.
6. Click *Save and apply changes*.

Configuring Boot Characteristics

By selecting the *Settings - Boot configuration* menu option, the administrative user can configure the MergePoint 5224/5240 SP Manager boot characteristics, including the location of the file from which the SP manager boots, whether or not the watchdog timer is active, the console speed and the speed of the Ethernet interfaces.

The Unit boot from pull-down menu lists the Network option, for booting from a TFTP boot server on the network, along with either one or two boot images that reside on the SP manager. A second image appears in the list only if the software has been upgraded. By default, the SP manager boots from an image file that resides on the on-board Flash memory.

CAUTION: Booting from the resident software is strongly recommended. Network boots should be reserved only for troubleshooting or upgrading.

Local boot options

To understand the local options on the Unit boot from menu, you need to understand how the MergePoint 5224/5240 SP manager handles software upgrades:

- The SP manager initially boots from a software image referred to as Image1.
- The first time a new software version is downloaded and installed, the new image is stored as Image2 in the Flash memory and the configuration is changed so the SP manager boots from image 2.
- The second time a new software version is downloaded and installed, the latest image is stored as Image 1, and the SP manager configuration is changed to boot from Image1.
- Subsequent downloads are stored following the same pattern, alternating Image1 with Image2.

In the Unit boot from pull-down menu, the entry for the current boot image is selected by default.

After a software upgrade, the boot file location choices are:

- Network

- Image1:*image_filename*
- Image2:*image_filename*

The word image is followed by the number, followed by a colon (:), followed by the name of the file, including the version number. The menu item has the following format:

`image1:zvmppconb.vversion_number`

The entry for the first release of the software, which is installed in the image1 area, is:

`image1:zvmppconb.v100`

After one or more software upgrades have been performed, a second image also appears in the menu, for example:

`image1:zvmppconb.v100`

`image2:zvmppconb.v101`

If you want to boot from another image than the one currently selected, you can select that image from the Unit boot from menu.

Network boot options

Network boots are recommended only for troubleshooting or for possible downloads of new software images that can then be stored in the resident removable Flash memory, as described in *To upgrade to a boot image from a network boot:* on page 204.

For network boot to work, make sure the following prerequisites are met.

- A TFTP server must be available to the SP manager.
- An upgraded boot image file must be available on the boot server.
- The SP manager must have a fixed IP address.

Table 5.1: Boot Configuration Fields and Options

Field or Value Name	Description
Appliance IP address	A new IP address for the SP manager.
Watchdog timer	Whether the watchdog timer is active. Choices are: • InActive • Active If the watchdog timer is active, the SP manager reboots if the software crashes. See *To configure boot:* on page 77 for how the watchdog timer can be activated or deactivated.
Unit boot from	Choose a local image or Network from the list.
Network boot file name	The name of the boot file being accessed over the network.
Server's IP address	The IP address for the boot server.

Table 5.1: Boot Configuration Fields and Options

Field or Value Name	Description
Console speed	An alternative console speed from 1200 to 115200.
eth0 fast ethernet	The speed of the eth0 interface • Auto Negotiation • 1000BaseT Full-Duplex • 100 BaseT Half-Duplex • 100BaseT Full-Duplex • 10BaseT Half-Duplex • 10BaseT Full-Duplex
eth1 fast ethernet	The speed of the eth1 interface • Auto Negotiation • 100 BaseT Half-Duplex • 100BaseT Full-Duplex • 10BaseT Half-Duplex • 10BaseT Full-Duplex

To configure boot:

1. Select the *Settings - Boot configuration* menu option. The Boot Configuration form appears.
2. Enter an IP address for the SP manager in the Appliance IP Address field.
3. Accept or change the option in the Watchdog Timer field (Inactive or Active).
4. Select the desired *Image* or *Network* from the Unit boot from menu.
5. If configuring network boot, perform the following steps:
   a. Accept or change the filename of the network boot program in the Network boot file name field. The file must be in the /tftpboot directory on the TFTP server specified in step b.
   b. Enter the IP address of the TFTP server in the Server's IP address field.
   c. Select a console speed from the Console speed pull-down menu.
6. Accept the default Auto Negotiation or select a speed for the eth0 interface from the eth0 fast ethernet pull-down menu.
7. Accept the default Auto Negotiation or select a speed for the eth1 interface from the eth1 fast ethernet pull-down menu.
8. Click *Save and apply changes.*

Configuring Outbound Email

By selecting the *Settings - Outbound email* menu option, the administrative user can configure an SMTP server and an email address for an administrator to receive email from the system, such as email generated by the cron daemon.

To configure a recipient for system email:

1. Select the *Settings - Outbound email* menu option. The Outbound email configuration screen appears.
2. Enter the email address in the System email forwarding address field.
3. Enter the DNS name or the IP address for the SMTP server.
4. Click *Save and apply changes.*

Configuring an Alternate Help File Location

By selecting the *Settings - Help* menu option, the administrative user can configure an alternate help file location, if it is desirable to make the help files available locally. The Help button on the Web Manager looks for help files at the URL specified on this screen.

An administrative user can change the location for the help files by first downloading the help files from the specified ftp server onto another web server or other directory that is available to users and then changing the URL in the URL Prefix field.

To specify a new location for help files:

1. Download the index.html and the compressed help files from ftp://ftp.cyclades.com/pub/cyclades/alterpath/mp5224_5240/doc/V_3.1.0. The file named 59E679501A.zip contains the installer and administrator help and the file named 59E675501A.zip contains the user help.
2. Create an mp5224_5240/V_3.1.0 subdirectory in the web server's root directory on a publicly accessible web server.

   ```
   # mkdir $<WEB_SERVER_ROOT>/mp5224_5240/V_3.1.0
   ```

3. In the V3.1.0 subdirectory, put the index.html file and extract the compressed installer and administrator help files. Subdirectories named admin/ and user/ are created for the help files.

   For example the following command line on a workstation running a UNIX-based operating system extracts the installer and administrator help file into an admin/ subdirectory.

   ```
   # cd $<WEB_SERVER_ROOT>/mp5224_5240/V_3.1.0
   # gunzip 59E679501A.zip
   ```

4. Log into the Web Manager as an administrative user, then select the *Settings - Help* menu option. The Help configuration screen appears.
5. In the URL prefix field, enter the new URL of the help files. The following example would work for a web server named remoteadmin where the index.html was installed into a mp5224_5240./V_3.1.0 directory at the web server's root.

   ```
   http://www.remoteadmin.com/mp5224_5240/V_3.1.0
   ```

NOTE: Make sure to not include a slash at the end of the URL

The software opens the index.html file, which contains links to the help files for the installer and administrator and the user.

6. Click *Save and apply changes.*

Configuring Target Devices

By selecting the *Config - Target Devices* menu option, the administrative user can configure target devices connected to the SP manager and configure data buffering. Target devices are defined using the values described in Table 4.15 on page 47.

The Data Buffering Default menu sets a default for data buffering for all devices, either Yes or No. When configuring individual devices, the administrative user can then select either Default, Yes or No to configure data buffering for the specific device. Selecting Default on this screen means that the data buffering value set on this page is used when the administrative user configures new target devices.

CAUTION: All devices connected to the private Ethernet ports of the SP manager must have a previously configured private subnet name assigned. If not, the device would only be accessible if connected to the public network, a highly unlikely scenario which is strongly discouraged.

The Web Manager displays target devices in the order in which they are configured. An administrator can configure target device lists to appear in alphabetical order using the cli utility. See *Changing the Sort Order of Device Listings* on page 132.

To configure data buffering for all target devices:

1. Select the *Config - Target Devices* menu option.
2. Select *Yes* or *No* from the Data buffering Default pull-down menu.
3. Click *OK*.
4. Click *Save and apply changes.*

Adding a target device

Make sure the following are complete.

- A private subnet has been created.
- An administrator has followed the procedure under *To find out if an existing command template works with a new target device:* on page 178 to find out if a default command template works with the new device. If a new template is needed, either the sptemplate utility can be used directly by an administrator as described under *To use the sptemplate utility to create a new template:* on page 178, or an administrative user can use the Web Manager configuration screen as described in *Configuring Target Device Types* on page 80.
- You know the username and password pair that are used for logging into the SP or other type of target device.

To add a target device:

1. Select the *Config - Target devices* menu option.
2. Click the *Add new target device* button.
3. Enter a descriptive name for a service processor or other type of target device in the Name field.
4. Enter the username and password pair used for logging into the device in the Login and Password fields and retype the password to verify.
5. If target device groups have been configured, select the device group from the Target device group pull-down menu.
6. Select a group from the Target device group pull-down menu if desired.

NOTE: For how to add a target device group, see *To configure device groups:* on page 83.

7. Select the target device type from the Type pull-down menu.
8. Select a data buffering option, *Yes*, *No* or *Default* from the Data buffering pull-down menu.
9. Select a private subnet name from the Private subnet pull-down menu.

NOTE: For how to configure private subnets, see *To configure a private subnet:* on page 106.

10. Enter the real IP address for the device in the Target Device IP address field.
11. If a virtual network has been configured as described in *Configuring virtual networks (DNAT)* on page 52, enter a virtual IP address for the device in the Virtual IP address field.
12. Enter a description in the Description field.
13. Select an authentication type from the Authentication type pull-down menu.
14. Select *Yes* or *No* from the Multisession pull-down menu (applies to SoL access only).
15. Click *OK*.
16. Click *Save and apply changes.*

Configuring Target Device Types

By selecting the *Config - Target device types* menu option, the administrative user can configure new target device types. A new target device type may be needed if a target SP does not work properly with any of the default types. New target device types are defined using the parameters and values described in Table 4.16 on page 49.

A new target device type may be configured in the following way on this screen.

- Start with one of the default types, and make modifications.
- Create a new target device template and then assign it to the SP.

One of the options is to change from Telnet to SSH as the connection protocol for communications with the target device type, which is done by selecting *ssh* from the Protocol pull-down menu.

CAUTION: For SSH tunneling between the SP manager and a target device to work, the SP manager's authentication method must match the authentication method assigned to the target device.

If the Configure target device templates button is clicked, a MindTerm session starts on the SP manager console, and it brings up the sptemplate utility. See *To use the sptemplate utility to create a new template:* on page 178. The new template is added to lists of command templates and becomes available for using when configuring target devices.

Configuring Users and Groups

By selecting the *Config - Users and groups* menu option, the administrative user can configure regular users and groups and authorize users and groups to access devices through the SP manager. An administrative user may also choose to configure users as administrative users by adding them to the admin group. Table 4.2 on page 25 shows the values to enter when configuring users.

Clicking the *Delete* button deletes the user or group without bringing up a confirmation dialog box.

Clicking the *Add* or *Edit* buttons for an existing user or group brings up a dialog for configuring users or groups. Clicking the *Device Access* button next to a user or group name brings up the Edit <user_or_groupname>'s dialog that shows any devices already assigned to the user or group; it also causes an *Add new device* button to appear, which brings up another dialog with the fields and menu options for configuring the access to a device. If no configured devices are available to be assigned, the *Add new device button* does not appear.

To create and authorize a user for target device management:

1. Select the *Config - Users and groups* menu option.
2. To add a user, perform the following steps:
   a. Click the *Add new user* button.
   b. Enter a username in the User Name field.
   c. Enter an identifying name and optional job description in the Full Name field.
   d. Select one of the radio buttons to choose a User Type:
   e. Enter a password in the Password field and re-enter it in the Retype password field.
   f. Select an option from the PPP/PPTP access pull-down menu: If you select any option except None from the PPP/PPTP access pull-down menu, enter a password in the PPP/PPTP password field and re-enter it in the Retype password field.
3. Assign target device access to a user by performing the following steps.
   a. Click the *Target device Access* button.
   b. Click the *Add new device* button. The Adding access to a new device for username screen appears.
   c. Select the target device from the New device pull-down menu.

d. Check the checkbox next to each device management action you wish to authorize the user to be able to perform on the selected target device.

e. Click *OK*. The Edit username's device access privileges screen appears.

4. Click *OK*.
5. Click *Save and apply changes*.

To modify a user's account:

1. Select the *Config - Users and groups* menu option.
2. Modify the user's name, role, description, and PPP/PPTP access by performing the following steps.
   a. Click the *Edit* button.
   b. If desired, change the username in the User Name field.
   c. If desired, change which radio button(s) is selected: Administrator or Normal user.
   d. If desired, change the full name and optional job description in the Full Name field.
   e. If desired, change the user's password in the Password field and re-enter it in the Retype password field.
   f. If desired, select an option or change which option is selected from the PPP/PPTP access pull-down menu.
   g. If you select any option except None from the PPP/PPTP access pull-down menu, enter a password in the PPP/PPTP password field and re-enter it in the Retype password field.
   h. Click *OK*.
3. Modify the user's device access by performing the following steps.
   a. Click the *Device Access* button.
   b. Click the *Add new device* button. The Adding access to a new device for username screen appears.
   c. Select the device from the New device pull-down menu.
   d. Check the checkbox next to each device management action you wish to authorize the user to be able to perform on the selected device.
   e. Click *OK*. The Edit <username's> device access privileges screen appears.
4. Click *OK*.
5. Click *Save and apply changes*.

To create and authorize user groups for target device management:

1. Select the *Config - Users and groups* menu option.
2. Add a group by performing the following steps.
   a. Click the *Add a new group* button.
   b. Enter a group name in the Group Name field.

c. Enter one or more members in the Members field.

Separate usernames with commas and no spaces.

d. Click *OK*. The Edit <groupname's> device access privileges screen appears.

3. Assign device access to a group by performing the following steps.
   a. Click the *Device Access* button on the line with the group name.
   b. Click the *Add new device* button.

      The Adding access to a new device for <groupname> screen appears.

   c. Select the device from the New device pull-down menu.
   d. Check the checkbox next to each device management action you wish to authorize the group to be able to perform on the selected device.
   e. Click *OK*. The Edit <groupname's> device access privileges screen appears.
4. Click *OK*.
5. Click *Save and apply changes*.

Configuring Device Groups

By selecting the *Config - Users and groups* menu option, the administrative user can configure optional groups of target devices to simplify target device configuration. If device groups are added, an administrator can add a new device to an existing group during configuration of the device. See *Configuring Target Devices* on page 79.

To configure device groups:

1. Select the *Config - Device groups* menu option.
2. Select *Add new group* or *Edit*.
3. Add or modify a device group by entering or modifying the group name and the description.
4. Click *OK*.
5. Click *Save and apply changes*.

Configuring Authentication Servers

By selecting the *Config - Authentication* menu option, the administrative user can configure authentication servers.

The default authentication type is Local, and if it is selected, it requires no configuration. If any other authentication method is selected, additional fields appear on the screen for specifying the information that is required to set up communications with an authentication server of the selected type.

When the administrative user configures an authentication server on this page, the server is available to perform authentication checking for logins to the following:

- Any target devices that are configured to use that authentication method. See *Configuring Target Devices* on page 79 for how devices are assigned an authentication method.
- The SP manager, if the SP manager is subsequently configured to use that authentication method. See *Configuring an Authentication Method for the MergePoint 5224/5240 SP Manager* on page 90 for how the SP manager is assigned an authentication method.

Configuring a Kerberos authentication server

By selecting the *Config - Authentication* menu option and selecting *Kerberos* from the Authentication Type pull-down menu, the administrative user can configure a Kerberos authentication server. Configure an authentication server when the SP manager or any of its target devices is configured to use the Kerberos authentication method or any of its variations (Kerberos, Local/Kerberos, Kerberos/Local or Kerberos Down/Local).

If the Kerberos authentication server (which is also referred to as a Key Distribution Center, or KDC) has previously been configured in either of the authentication configuration screens, the fields are filled in with the previously configured values.

Before configuring a Kerberos server, the administrative user must obtain from the server's administrator the Kerberos Realm Domain Name and the Kerberos Server IP address.

CAUTION: The Kerberos KDC rejects tickets when the timestamp on an authentication request from a host is not within the maximum clock skew time specified in the KDC's hdc.conf file. Therefore, it is essential for the time on the SP manager to be synchronized with the time on the KDC.

Also, work with the Kerberos server's administrator to ensure that following types of accounts are set up on the Kerberos server and that the administrators of the SP manager and target devices know the passwords assigned to the accounts:

- An account for admin or other administrative user
- If Kerberos authentication is specified for the SP manager, accounts for all users who need to log into the SP manager to administer target devices
- If Kerberos authentication is specified for devices, accounts for users who need access to target devices

To configure a Kerberos authentication server:

1. Make sure entries for the appliance and the Kerberos server exist in the SP manager's /etc/hosts file.
   a. Select the *Network - Host Table* menu option. The Host Table form appears.
   b. Add an entry for appliance (if needed) and add an entry for the Kerberos server.
2. Make sure that timezone and time and date settings are synchronized between the SP manager and on the Kerberos server.

NOTE: Kerberos authentication depends on time synchronization. Time and date synchronization is most easily achieved by setting both the SP manager and the Kerberos server to use the same NTP server.

a. Follow the procedure under *Configuring System Date and Time* on page 74 to set the timezone, date and time.

b. Work with the authentication server's administrator to synchronize the time and date between the SP manager and the server.

3. Select the *Config - Authentication* menu option.
4. Select *Kerberos* from the Authentication Type pull-down menu. The Kerberos configuration fields display.
5. Enter the IP address of the Kerberos server in the Kerberos Server IP address field.
6. Enter the domain name of the Kerberos realm in the Kerberos Realm Domain Name field.
7. Click *Save and apply changes.*

Configuring an LDAP authentication server

By selecting the *Config - Authentication* menu option and selecting *LDAP* from the Authentication Type pull-down menu, the administrative user can configure an LDAP authentication server. Configure an authentication server when the SP manager or any of its target devices is configured to use the LDAP authentication method or any of its variations (Local/LDAP, LDAP/Local or LDAP Down/Local).

The following two fields and menu display when the LDAP authentication type is selected:

- LDAP Server IP address
- LDAP Base - The distinguished name of the search base

  The default distinguished name is dc, as in dc=value,dc=value. For example, if the distinguished name on the LDAP server is o, then replace dc in the base field with o, as in o=value,o=value.

  The domain name is specified as shown in the following example. For the LDAP domain name cyclades.com, the correct entry would be: dc=cyclades,dc=com.

- Secure LDAP pull-down menu. Options are Off, On and Start TLS

You can enter information in the following three fields, but entries are not required:

- LDAP User Name
- LDAP Password
- LDAP Login Attribute (defaults to UID)

Work with the LDAP server's administrator to ensure that following types of accounts are set up on the LDAP server and that the administrators of the SP manager and target devices know the passwords assigned to the accounts:

- An account for admin or other administrative user.
- If LDAP authentication is specified for the SP manager, accounts for all users who need to log into the SP manager.
- If LDAP authentication is specified for devices, accounts for users who need access to the target devices.

See *Configuring group authorization for LDAP authentication* on page 133 for how to manually configure group authorizations with LDAP authentication, if desired.

To configure an LDAP authentication server:

1. Select the *Config - Authentication* menu option.
2. Select *LDAP* from the Authentication Type pull-down menu. The LDAP form displays with LDAP Server and LDAP Base fields filled in from the current values in the /etc/ldap.conf file.
3. Enter the IP address of the LDAP server in the LDAP Server field.
4. If the LDAP authentication server uses a different distinguished name for the search base than the one displayed in the LDAP Base field, change the definition.
5. Replace the default domain name with the name of your LDAP domain.
6. Pick an option from the Secure LDAP pull-down menu.
7. Enter an optional username in the LDAP User Name field.
8. Enter an optional password in the LDAP Password field.
9. Enter an optional login attribute in the LDAP Login Attribute field.
10. Click *Save and apply changes*. The changes are stored in /etc/ldap.conf on the SP manager.

Configuring a NIS authentication server

By selecting the *Config - Authentication* menu option and selecting *NIS* from the Authentication Type pull-down menu, the administrative user can configure a NIS authentication server.

Configure a NIS authentication server when the SP manager or any of its target devices is configured to use the NIS authentication method or any of its variations (NIS/DownLocal, Local/NIS or NIS/Local).

The administrative user must obtain the needed NIS Domain Name and NIS Server IP address from the server's administrator.

Work with the NIS server's administrator to ensure that the following types of accounts are set up on the NIS server and that the administrators of the SP manager and target devices know the passwords assigned to the accounts:

- An account for admin
- If NIS authentication is specified for the SP manager, accounts for all users who need to log into the SP manager

- If NIS authentication is specified for devices, accounts for users who need access to the target devices

To configure a NIS authentication server:

1. Select the *Config - Authentication* menu option.
2. Select *NIS* from the Authentication Type pull-down menu. The NIS fields display.
3. Enter the NIS domain name in the NIS Domain Name field.
4. Enter the IP address of the NIS server in the NIS Server IP field.
5. Click *Save and apply changes.*

Configuring a RADIUS authentication server

By selecting the *Config - Authentication* menu option and selecting *RADIUS* from the Authentication Type pull-down menu, the administrative user can configure a RADIUS authentication server. Configure a RADIUS authentication server when the SP manager or any of the target devices is configured to use the RADIUS authentication method or any of its variations (Local/Radius, Radius/Local or Radius Down/Local).

The administrative user must obtain the needed information about the RADIUS server from the server's administrator:

- First Authentication Server
- Second Authentication Server
- First Accounting Server
- Second Accounting Server
- Secret
- Timeout(s)
- Retries

Work with the RADIUS server's administrator to ensure that following types of accounts are set up on the RADIUS server and that the administrators of the SP manager and target devices know the passwords assigned to the accounts:

- An account for admin or other administrative user.
- If RADIUS authentication is specified for the appliance, accounts for all users who need to log into the SP manager.
- If RADIUS authentication is specified for devices, accounts for users who need access to the target devices.

See *Configuring group authorization for RADIUS authentication* on page 136 for how to manually configure group authorizations with RADIUS authentication.

To configure a RADIUS authentication server:

1. Select the *Config - Authentication* menu option.

2. Select *Radius* from the Authentication Type pull-down menu.
3. Enter the IP address of the first or only authentication server in the First Authentication Server field.
4. Enter the IP address of a second authentication server (if available) in the Second Authentication Server field.
5. Enter the secret in the Secret field.
6. Enter one or more time-out values in the Timeout field.
7. Enter a number of retries in the Retries field.
8. Click *Save and apply changes.*

Configuring an SMB authentication server

By selecting the *Config - Authentication* menu option and selecting *SMB* from the Authentication Type pull-down menu, the administrative user can configure an SMB authentication server. Configure an SMB authentication server when the SP manager or any of the target devices is to use the SMB authentication method or any of its variations (Local/SMB, SMB/Local or SMB Down/Local).

The administrative user must obtain from the server's administrator the needed Domain, Primary Domain Controller and Secondary Domain Controller information.

Work with the SMB server's administrator to ensure that the following types of accounts are set up on the SMB server and that the administrators of the SP manager and target devices know the passwords assigned to the accounts:

- An account for admin or other administrative user
- If SMB authentication is specified for the SP manager, accounts for all users who need to log into the SP manager
- If SMB authentication is specified for devices, accounts for users who need access to the target devices

To configure an SMB authentication server:

1. Select the *Config - Authentication* menu option.
2. Select *SMB* from the Authentication Type pull-down menu.
3. Enter the SMB domain name in the Domain field.
4. Enter the IP address of the primary domain controller in the Primary Domain Controller field.
5. Enter the IP address of the secondary domain controller in the Secondary Domain Controller field.
6. Click *Save and apply changes.*

Configuring a TACACS+ authentication server

By selecting the *Config - Authentication* menu option and selecting *TACACS+* from the Authentication Type pull-down menu, the administrative user can configure a TACACS+ authentication server. Configure a TACACS+ authentication server when the SP manager or any of the target devices is to use the TACACS+ authentication method or any of its variations (Local/ TACACS+, TACACS+/Local or TACACS+ Down/Local).

The administrative user must obtain the following needed information about the TACACS+ server from the server's administrator:

- First Authentication Server
- Second Authentication Server
- First Accounting Server
- Second Accounting Server
- Secret
- Enable Raccess Authorization
- Timeout(s)
- Retries

Prerequisites for a TACACS+ server configuration

To configure a TACACS+ authentication server, you must prepare for the following:

- An account for admin or other administrative user.
- If TACACS+ authentication is specified for the SP manager, accounts for all users who need to log into the SP manager.
- If TACACS+ authentication is specified for devices, accounts for users who need access to the target devices.

To configure a TACACS+ authentication server:

1. Select the *Config - Authentication* menu option.
2. Select *TACACS+* from the Authentication Type pull-down menu.
3. Enter the IP address of the first authentication server in the First Authentication Server field.
4. Enter the IP address of a second authentication server in the Second Authentication Server field.
5. Enter the IP address of the first accounting server in the First Accounting Server field.
6. Enter the IP address of the second accounting server in the Second Accounting Server field.
7. Enter the secret in the Secret field.
8. Check or leave unchecked the *Enable Raccess Authorization* checkbox.
9. Enter one or more time-out values in the Timeout field.

10. Enter a number of retries in the Retries field.
11. Click *Save and apply changes.*

Configuring an Authentication Method for the MergePoint 5224/5240 SP Manager

By selecting the *Config - Unit Authentication* menu option, the administrative user can configure the authentication method that applies when anyone attempts to log into the MergePoint 5224/5240 SP manager.

By default, Local authentication is in effect and no configuration is required.

The specified type of authentication server must be available and must be configured as described under *Configuring Authentication Servers* on page 83.

To configure an authentication method for SP manager logins:

1. Select the *Config - Unit authentication* menu option.
2. Select the desired authentication type from the Authentication Type pull-down menu.
3. Click *Save and apply changes.*

Configuring Notifications

By selecting the *Config - Notifications* menu option, the administrative user can define alarm triggers to generate notifications when specified events occur. The syslogd filters logs for the specified kinds of messages and takes action based on the content of the messages. The administrative user specifies the notices to be sent either by SNMP trap, pager or email.

To configure a notification, the administrative user clicks the *Add* button after selecting one of the notification methods from the menu. The dialog that appears next has different fields and menu options depending on which notification method is selected.

The following table shows the fields for configuring any type of notification.

Table 5.2: Values for Configuring Any Type of Notification

Checkbox, Field or Menu Name	Description
Scan device console session for matches	As stated
Name	The name for the trigger
Alarm trigger	A function and a regular expression in syslog-ng format. Use the format: function('regular_expression'). For example, the following example searches system messages for Denied, denied, Fail and fail: match('[Dd]enied | [Ff]ail'); See *MergePoint 5224/5240 SP Manager Notifications* on page 43 for more format examples.

Configuring SNMP trap notifications

If the Simple Network Management Protocol (SNMP) service is enabled on the SP manager, the administrative user can use the SNMP Trap Add dialog to send notifications about significant events to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

The SNMP Trap Add dialog may be used for configuring an alarm trigger and a SNMP trap notification to be sent if the specified alarm trigger occurs.

To configure SNMP trap notifications:

1. Select the *Config - Notifications* menu option.
2. Select *SNMP trap* from the pull-down menu.
3. Select *Add*.
4. Check or leave unchecked the checkbox next to *Scan target device console session for matches*.
5. Enter a name for the trigger in the Name field.
6. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
7. Select a protocol from the Protocol menu.
8. Enter an OID in the OID field.
9. Select one of the trap designators from the Generic trap type pull-down menu. If the enterpriseSpecific trap designator is selected, you are prompted for a specific trap number.
10. If either SNMP v1 or v2c is selected, enter a community name in the Community field.
11. If SNMP v3 is selected, perform the following steps:
    a. Enter a username in the User field.
    b. Select an authentication level from the Auth Level pull-down menu.
    c. If Auth or Auth & crypt are selected, select an option from the Auth Level menu.
    d. Enter an optional password in the Auth password field.
    e. If Auth & crypt is selected, select an option from the Encryption menu.
    f. Enter an optional password in the Crypt password field.
12. Enter an SNMP server IP address or DNS name in the SNMP server field.
13. Enter any desired text in the Body field.
14. Click *OK*.
15. Click *Save and apply changes.*

Configuring pager notifications

The administrative user can use the Pager Add dialog to configure an alarm trigger and a pager notification to be sent if the specified alarm trigger occurs. For pager notifications, the administrative user must configure the values in Table 5.3, in addition to the values in Table 5.2 on page 90.

Table 5.3: Fields for Configuring a Pager Notification

Field or Menu Name	Notes
Pager/phone number	The pager or phone number to receive the notification
Text	The text to be sent in the trap message
SMS username	The Short Message Services (SMS) username
SMS server	The SMS server's IP address or DNS name
SMS port	The SMS port number

To configure pager notifications:

1. Select the *Config - Notifications* menu option.
2. Select *Pager* from the pull-down menu.
3. Select *Add*.
4. Check or leave unchecked the checkbox next to *Scan device console session for matches*.
5. Enter a name for the notification in the Name field.
6. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
7. Enter a pager or phone number in the Pager/phone number field.
8. Enter the desired text in the Text field.
9. Enter a username in the SMS username field.
10. Enter the IP address for an SMS server in the SMS server field.
11. Enter an SMS port in the SMS port field.
12. Click *OK*.
13. Click *Save and apply changes*.

Configuring email notifications

The administrative user can use the Email Add dialog to configure an alarm trigger and an email notification to be sent if the specified alarm trigger occurs. For email notifications, the administrative user must configure the values in Table 5.4 in addition to the values in Table 5.2 on page 90.

Table 5.4: Fields for Configuring an Email Notification

Field or Menu Name	Notes
To	The email address of the user account to receive the notification
From	The sender's email address
Subject	Summary text to describe the event triggering the email
Body	Description of the event

To configure an email notification:

1. Select the *Config - Notifications* menu option.
2. Select *Email* from the pull-down menu.
3. Select *Add*.
4. Check or leave unchecked the checkbox next to *Scan device console session for matches*.
5. Enter a name for the notification in the Name field.
6. Use syslog-ng syntax to specify an event to trigger the alarm in the Alarm trigger field.
7. Enter a destination email address in the To field.
8. Enter a source email address in the From field.
9. Enter a subject that describes the alarm trigger in the Subject field.
10. Enter the desired text for the email message in the Body field.
11. Click *OK*.
12. Click *Save and apply changes*.

Configuring Sensor Alarms

By selecting the *Config - Sensor alarms* menu option, the administrative user can configure the SP manager to check sensor readings from SPs and to configure alarms to be sent if the sensor readings are not within certain specified values.

To begin configuring a sensor alarm:

1. Select the *Config - Sensor Alarms* menu option.
2. Click the *Add new alarm* button. The add sensor alarm dialog appears.

3. Select a target device from the Device pull-down menu.
4. Specify the sensor to monitor in the Sensor field.
5. Select a condition to trigger the sensor alarm from the Condition pull-down menu.
6. When the condition selected in step 5 is inside or outside a range, specify the range in the Range fields.
7. Specify a polling interval and choose minutes or hours from the Interval pull-down menu.
8. Select the desired notification action from the Action pull-down menu.
9. Enter a comment, if desired, in the Comment field.

Configuring a syslog message sensor alarm action

By selecting the *Config - Sensor alarms* menu option and selecting *Syslog Message*, the administrative user can configure syslog message sensor alarms.

To configure a Syslog message sensor alarm action:

1. Select the *Config - Sensor Alarms* menu option.
2. Select *Syslog message* from the Action menu.
3. Select a priority from the Priority menu.
4. Enter text as desired in the Body field.
5. Click *OK*.
6. Click *Save and apply changes*.

Configuring the SNMP trap sensor alarm action

By selecting the *Config - Sensor alarms* menu option and selecting *SNMP trap*, the administrative user can configure SNMP trap notifications. See *SNMP on the MergePoint 5224/5240 SP Manager* on page 29 for values to define SNMP traps.

To configure an SNMP trap sensor alarm action:

1. Select the *Config - Sensor Alarms* menu option.
2. Select *SNMP trap* from the Action menu.
3. Select a protocol from the Protocol menu.
4. Enter the OID in the OID field.
5. Select a trap type from the Generic trap type field.
6. If either v1 or v2 is selected in step 5, enter the name of a community in the Community field.
7. If v3 is selected in step 5, perform the following steps:
    a. Enter the username required for authentication in the User field.
    b. Select an authentication level from the Auth Level pull-down menu.
    c. If Auth or Auth & Crypt are selected, select an authentication method from the Auth Method pull-down menu.

d. If Auth or Auth & Crypt are selected, enter the authentication password in the Auth password field.
e. If Auth & Crypt is selected, select an encryption method from the Encryption pull-down menu.
f. If Auth & Crypt is selected, enter the appropriate password for the encryption method in the Crypt pass field.
g. Enter the IP address or DNS-resolvable name of the SNMP manager in the Server field.
h. Enter any desired text in the Body field.

8. Click *OK*.
9. Click *Save and apply changes*.

Configuring a pager sensor alarm action

By selecting the *Config - Sensor alarms* menu option and selecting *Pager*, the administrative user can configure pager notifications.

Table 5.5: Fields for Configuring Pager Sensor Alarms

Field or Menu Name	Notes
Pager/phone number	Pager or phone number.
SMS username	SMS username.
SMS server	SMS server IP address.
SMS port	Port number.
Message	Any desired text to include with the pager message.

To configure a pager sensor alarm action:

1. Select the *Config - Sensor Alarms* menu option.
2. Select *Pager* from the Action menu.
3. Enter the phone number of the pager or phone to be contacted in the Pager/phone number field.
4. Enter the username required for authentication in the SMS username field.
5. Enter the IP address of the SMS server in the SMS server field.
6. Enter the SMS port number in the SMS port field.
7. Enter any desired message in the Message field.
8. Click *OK*.
9. Click *Save and apply changes*.

Configuring an email sensor alarm action

By selecting the *Config - Sensor alarms* menu option and selecting *Email*, the administrative user can configure email notifications.

Table 5.6: Fields for Configuring Email Sensor Alarms

Field or Menu Name	Notes
From:	Identifies the sender, for example root@MergePoint5224.
To:	Designates who is to receive the email.
Subject:	Identifies the source of the message, for example: Alarm: Sensor Error from rack1_dev2_ilo.
Body	Any desired text to include with the email message.

To configure an email sensor alarm action:

1. Select the *Config - Sensor Alarms* menu option.
2. Select *Email* from the Action menu.
3. Enter the sender's email address in the From field.
4. Enter the recipient's email address in the To field.
5. Enter a string that identifies the alarm in the Subject field.
6. Enter an explanatory message for the alarm in the Body field.
7. Click *OK*.
8. Click *Save and apply changes*.

Configuring SNMP

By selecting the *Config - SNMP* menu option, the administrative user can configure SNMP access for the SP manager and for target devices.

NOTE: For SNMP to work you need to need to ensure that the selected security profile enables the SNMP service (by checking the Config - Security profile screen) or that the SNMP service is active (by checking the Config - Services screen). If the security profile in effect enables SNMP, you do not need to activate SNMP on the Services screen.

Administrative users can enable notifications about significant events occurring on target devices to be sent from the SP manager to an SNMP management application, such as HP Openview, Novell NMS, IBM NetView or Sun Net Manager.

To configure appliance SNMP information:

1. Select the *Config - SNMP* menu option.
2. Click the *Edit* button.

3. Accept or change the text in the Contact field.
4. Accept or change the location in the Location field.
5. Click *OK*.
6. Click *Save and apply changes.*

To begin configuring SNMP for a device:

1. Log into the Web Manager as an administrative user.
2. Select the *Config - SNMP* menu option and the Access tab.
3. Click the Configure button next to the name of the device to configure. The Target Device Device <devicename> SNMP settings window appears.

To configure a device's SNMP access settings:

1. Select a device to configure on the Config - SNMP - Access page, as described under *To begin configuring SNMP for a device:* on page 97.
2. Click *Edit* under the Service Processor SNMP setting heading. The Target Device <devicename> SNMP settings dialog appears.
3. Enter the identifier for the object to be managed in the OID field.
4. Select a version from the SNMP version pull-down menu.
5. If either the v1 or v2c version is selected in step 4, enter a community name in the Community field.

   -or-

   If the v3 version is selected in step 4, perform the following steps:

   a. Enter the username required for authentication in the User name field.
   b. Select an authentication method from the Auth method pull-down menu.
   c. Enter an optional authentication password in the Auth pass field.
   d. Select an encyrption method from the Encryption pull-down menu.
   e. Enter an optional encryption password in the Crypt pass field.
6. Click *OK*.

To configure users' SNMP access settings:

Perform this procedure to configure how users on the public side authenticate themselves to the SP manager, whether they are using SNMP functionality on the SP manager itself or SNMP functionality proxied from the device.

1. Select a device to configure on the Config - SNMP - Access page, as described under *To begin configuring SNMP for a device:* on page 97.
2. Click the *Add access* button under the SNMP access settings heading. The Target Device -<*devicename*> - SNMP access configuration screen appears.

3. Select a version from the SNMP version pull-down menu.
4. If the v3 version is selected in step 3, go to *To configure users with SNMP v3:* on page 98. If either the v1 or v2c version is selected in step 3, perform the following steps:
   a. Enter a community name in the Community field.
   b. Select a Source radio button, either Default or Use IP.
   c. If *Use IP* is selected, enter a source IP address.
   d. If a view has been configured, select a Read view and Write view from the Security level pull-down menus. If no view has been configured, go to *To configure views with SNMP v3:* on page 98.
5. Click *OK*.
6. Click *Save and apply changes.*

To configure users with SNMP v3:

If the v3 version is selected in step 3 of the previous procedure, configure users as desired by clicking the Add user button. The User configuration dialog appears.

1. Click the *Add user* button. The User settings dialog appears.
2. Enter a username in the User name field.
3. Select an authentication method from the Auth method menu.
4. Enter an optional authentication password in the Auth pass field.
5. Select an encryption method from the Encryption menu.
6. Enter an optional encryption password in the Crypt pass field.
7. Click *OK*.
8. Click *Save and apply changes.*

To configure views with SNMP v3:

1. Click the *Edit views* button. The Views configuration dialog appears.
2. Click the *Add View* button. The SNMP view settings dialog appears.
3. Enter a name for the view in the View name field.
4. Enter an OID for the object to be viewed in the OID field.
5. If desired, enter a Mask to create a OID subtree.
6. If desired, exclude the defined OID subtree by selecting the *Exclude* option from the left menu.
7. Click *OK*.
8. Click *Save and apply changes.*

To configure security with SNMP v3:

1. Select a read view and write view from the No auth menus under the Read view and Write view columns.

2. Select a read view and write view from the Auth menus under the Read view and Write view columns.
3. Select a read view and write view from the Auth & crypt menus under the Read view and Write view columns.
4. Click *OK*.
5. Click *OK*.
6. Click *Save and apply changes*.

To configure SNMP trap forwarding:

1. Select the *Config - SNMP* menu option.
2. Click the *Add trap* button under the Trap forward configuration heading.
3. Enter an optional IP address in the Source IP address field.
4. Enter the IP address of the SNMP server to receive the trap in the Destination IP address field.
5. Enter the OID of the device in the OID field.
6. Click *OK*.
7. Click *Save and apply changes*.

Configuring Logging of System Messages (Syslogs)

By selecting the *Config - Syslog* menu option, the administrative user can configure system logs. See *Message Logging (With Syslog) on the MergePoint 5224/5240 SP Manager* on page 38 for more details.

To configure the Syslog destination and message filtering:

1. Select the *Config - Syslog* menu option. The Syslog screen displays.
2. To configure messages to be sent to the console, click the *Console* checkbox.
3. To configure messages to be sent to the root user, click the *Root user* checkbox.
4. To configure messages to be sent to a syslog server, add a syslog server to the Syslog servers list by performing the following steps.
    a. Enter a syslog server’s IP address in the New syslog server field.
    b. Click the *Add* button.
    c. To add additional syslog servers, repeat steps a and b.
5. On the Filter web log messages by level screen, specify which types of web log messages are forwarded by clicking the checkboxes next to the desired severity levels.
6. On the Filter system log messages by level screen, specify which types of system log messages are forwarded by clicking the checkboxes next to the desired severity levels.
7. Click *Save and apply changes*.

Configuring the Event Log Backend

By selecting the *Config - Event log backend* menu option, the administrative user can configure event logging for connected service processors.

To configure system event logging for connected SPs:

1. Select the *Config - Event log backend* menu option. The Event log backend profile screen appears.
2. Click the *Edit* button to edit event logging for a device. The Edit <device_name> Event Log Settings for Device appears.
3. Select *On* or *Off* from the Logging Status pull-down menu or accept the currently selected menu option.
4. Change or accept the number in the Read Frequency field, select Hours or Minutes from the pull-down menu or accept the currently selected menu option.
5. Change or accept the number of bytes in the Max Log Size (Bytes) field.
6. Click *OK*.
7. Click *Save and apply changes.*

Selecting or Configuring a Security Profile

By selecting the *Config - Security profile* menu option, the administrative user can select one of the default security profiles or configure a custom security profile for the SP manager. For more details about the services and features configured by default security profiles and what you can change in a custom profile, see *Security Profiles* on page 25.

The Moderate profile is the default option selected on the Security level menu.

NOTE: Changing the security profile can disable or enable services that may have been turned on or off by some other means.

See Chapter 4 for the features in the Moderate, Secured and Open security profiles.

NOTE: If you select the secured profile, HTTP is disabled by the secured security profile. Follow the reminder at the bottom of the screen by making sure to notify all users that they must use HTTPS when bringing up the Web Manager.

To select or customize the security profile:

1. Select the *Config - Security profile* menu option. The Security profile screen displays.
2. Click the *Proceed* button.
3. Select a security profile from the Security Level pull-down menu.

4. If you select the *Custom* profile, make sure the checkboxes are checked next to services and features you want to be enabled and make sure the checkboxes are clear next to services and features you want to be disabled.
5. Click *OK*. The security profile confirmation screen appears.
6. Click *Save and apply changes*.

To configure services:

1. Select the *Config - Services* menu option. The Config - Services screen appears with checkmarks next to the services that have been enabled by default.
2. Enable or disable any of the listed network services by checking the checkboxes next to the corresponding service.
3. Click *Save and apply changes* to enable or disable any selections.

Configuring Network Interfaces

By selecting the *Config - Network - Host settings* menu option, the administrative user can configure the MergePoint 5224/5240 SP manager's network interfaces and can configure DNS for the SP manager.

Table 4.11 on page 40 shows the values to configure for network interfaces. Table 4.12 on page 41 shows the values to use when configuring Ethernet ports.

When configuring public Ethernet ports, be aware of the following:

- When DHCP is enabled for an interface and the DHCP server cannot be reached for any reason, the interface IP address falls back to the factory default static IP address (192.168.160.10) unless an administrator has assigned another IP address to the interface.
- When both interfaces are active and assigned two different IP addresses, both interfaces are reachable through either IP address even if the cable is disconnected from one of the interfaces.

With failover enabled, the secondary Ethernet interface becomes bonded to the primary Ethernet interface, and the bonded interfaces are referred to as a single bond0 interface. As a result, the same set of values applies to the single bond0 interface.

Configuring primary and secondary Ethernet ports

If failover is disabled, the administrative user can configure each Ethernet port separately in the following ways:

- Enable or disable each Ethernet port
- Enable or disable DHCP
- If DHCP is disabled, configure each port for static IP addressing

To configure the network interfaces:

1. Select the *Network - Host settings* menu option.

2. Modify the name in the Host name field, if desired.
3. Enable or disable failover by selecting the desired option from the Failover pull-down menu.
4. Enable DHCP, if desired, by making sure the *DHCP* checkbox is checked.
5. If DHCP is not enabled, configure a static IP address for an Ethernet port by performing the following steps.
   a. Disable DHCP by making sure the *DHCP* checkbox is not checked.
   b. Enter or modify the IP address in the IP address field.
   c. Enter or modify the netmask in the Network Mask field.
   d. Enter or modify the IP address for a network gateway in the Gateway IP field.

NOTE: The IP address entered in the Gateway IP field is used for the SP manager's default route.

   e. Enter or modify a broadcast IP address in the Broadcast field.
   f. Enter or modify the maximum transmission unit value for the Ethernet port in the MTU field.
6. Configure DNS, if desired, by performing the following steps.
   a. Enter or modify the IP address for a primary DNS server in the Primary DNS field.
   b. Enter or modify the IP address for an optional secondary DNS server in the Secondary DNS field.
   c. Enter or modify an existing domainname in the Domain name field.
7. Click *Save and apply changes.*

Configuring Firewall Rules for Packet Filtering

By selecting the *Network - Firewall* menu option, the administrative user can configure packet filtering.

The Network - Firewall screen provides an interface to iptables. Six built-in chains are pre-configured with hidden rules. Using this screen, an administrative user can define rules for the built-in chains. Once rules have been administratively defined, they can be edited or deleted.

The top three chains shown on the screen are defined in the iptables filter table and the bottom three chains are defined in the iptables nat table. An *Add new <table_name> <chain_name >* rule button appears under the entry for each chain, for example the Add new NAT prerouting rule button appears under the entry for the nat PREROUTING chain.

Administrative users may want to add rules to the default chains to suit their environment and their needs. Whenever a rule is added, a number is assigned automatically, starting with 0. An Edit and a Delete button appear next to the entry for each administrator-defined rule.

To add a new packet filtering (firewall) rule:

1. Select the *Network - Firewall* menu option.

2. Click the *Add new <table_name> <chain_name >* rule button underneath the entry for the chain to which you wish to add a rule.
3. Configure one or more of the following filtering options, as desired.
   a. Select a protocol from the Protocol pull-down menu.
   b. Specify a source IP and subnet mask in the form: *hostIPaddress or networkIPaddress/NN.*
   c. Specify a destination IP and subnet mask in the form: *hostIPaddress* or *networkIPaddress/NN.*
   d. Depending on which chain you selected, select an input or output interface from the Input interface or Output interface pull-down menu.
   e. Choose the types of packets to be filtered from the Fragments pull-down menu.
   f. Select a target from the Rule target pull-down menu.
4. Click *OK.*
5. Click *Save and apply changes.*

To edit an administrator-added packet filtering (firewall) rule:

1. Select the *Network - Firewall* menu option.
2. Click the *Edit* button for the entry for the rule you want to change.
3. Configure one or more of the following filtering options, as desired.
   a. Select or accept the protocol selected from the Protocol pull-down menu.
   b. Accept or change the value entered in the Source IP/mask field, using the form: *hostIPaddress* or *networkIPaddress/NN,* where *NN* is the subnet length.
   c. Accept or change the value entered in the Destination IP/mask in the form: *hostIPaddress networkIPaddress/NN,* where *NN* is the subnet length.
   d. Depending on which type of chain is selected, accept or change either the input or output interface selected from the Input interface or Output interface pull-down menu.
   e. Accept or change the types of packets to be filtered selected from the Fragments pull-down menu.
   f. Accept or change the target selected from the Rule target pull-down menu.
4. Click *OK.*
5. Click *Save and apply changes.*

Configuring Hosts

By selecting the *Network - Host table* menu option, the administrative user can configure hosts.

To add a new host:

1. Select the *Network - Host* menu option.
2. Enter an IP address in the IP address field.

3. Enter a hostname in the Name field.
4. (Optional) Enter an alias for the host.
5. Click *OK*.
6. Click *Save and apply changes*.

Configuring Static Routes

By selecting the *Network - Static routes* menu option, the administrative user can either manually add a static route or to edit or delete existing static routes.

Table 5.7: Fields and Menus for Configuring Static Routes

Field or Menu Name	Definition
Network Address	Enter the IP address of the destination host or specify a network in the form *networkIPaddress*/*mask_length* (also referred to as prefix/length). **NOTE:** To set a default route, select *Network - Host Settings*.
Type	Select Gateway or Interface.

Interface/Gateway	• When Interface is selected from the Type menu, the Interface/Gateway menu choices are:
	  • Public 1
	  • Public 2
	  • Failover
	  • PCMCIA 1
	  • PCMCIA 2
	• When *Gateway* is selected from the Type menu, a field appears for entering the IP address of the gateway.

Metric	Enter the number of hops to the destination.

To add a static route:

1. Select the *Network - Static routes* menu option.
2. Enter a network IP address in the Network Address field.
3. Select Interface or Gateway from the Type pull-down menu.
4. Enter the number of hops to the destination in the Metric field.
5. Click *Apply*.
6. Click *Save and apply changes*.

Configuring VPN Connections

In order to enable authorized users to access native IP management features on an SP, an administrative user must configure a VPN connection on the user's side and the SP manager side.

By selecting the *Network - VPN connections* menu option, the administrative user can perform the following tasks on the SP manager:

- Configure one or more IPSec VP connections.
- Configure a single PPTP VPN connection with a pool of IP addresses.

Table 4.10 on page 37 describes the fields for configuring a PPTP profile. Specify a pool of addresses in the form 10.0.0.100-110.

To configure IPSec VPN:

1. Select the *Network - VPN connections* menu option.
2. Click *Add new connection*.
3. The IPSec VPN Connection Configuration dialog appears.
4. Enter any descriptive name you choose for the connection in the Connection name field.
5. Select either *ESP* or *AH* from the Authentication protocol pull-down menu.
6. Select *Shared Secret* or *RSA public keys* from the Authentication method pull-down menu.
7. If *Shared secret* is selected, enter the shared secret in the Pre-Shared key field.
8. Set up the right and left hosts by performing the following steps.
    a. Enter the name of the SP manager (left host) or the remote computer (right host) in the ID field.
    b. Enter the IP address of the SP manager (left host) or the remote computer (right host) in the IP Address field.
    c. Enter the IP address of the router through which the host's packets reach the Internet in the NextHop field.
    d. Enter the netmask for the subnet in the Subnet Mask field.
9. If RSA public keys is selected in step 6, perform one of the following steps.
    a. When configuring the left host, generate the key for the SP manager and use copy and paste to enter the key in the RSA key field.
    b. When configuring the right host, find out the key from the remote gateway (where the right host resides) and enter the key in the RSA key field.
10. Select either *Ignore*, *Add*, *Add and route* or *Start* from the Boot Action pull-down menu.
11. Click *OK*.
12. Click *Save and apply changes*.

To configure a PPTP VPN connection:

1. Select the *Network - VPN connections* menu option.
2. Enter a single IP address or a pool of IP addresses in the PPP local address pool field.
3. Enter a single IP address or a pool of IP addresses in the PPP remote address pool field.
4. Click *Save and apply changes*.

5. Make sure that users who are authorized for native IP are also authorized for PPTP connections.

Configuring Private Subnets and Virtual Networks

By selecting the *Network - Private subnets* menu option, the administrative user can configure private subnets and optional virtual (DNAT) networks, based on a predefined addressing scheme. Deciding which addressing scheme to use is discussed in *Private Subnets and Virtual DNAT Networks on the MergePoint 5224/5240 SP Manager* on page 50 and in more detail in *Target Device Configuration* on page 169.

At least one subnet is needed to enable devices that are connected to the SP manager's private Ethernet ports to communicate on the Internet via the SP manager's public IP address. Any number of private subnets may be configured. Virtual networks configuration is optional.

Subnets are defined using the values described in Table 4.17 on page 51.

Virtual networks are defined using the values described in Table 4.18 on page 52.

CAUTION: Changing or deleting an existing private subnet changes the configuration of any device that was previously configured to use that private subnet; the private subnet is removed from the device's configuration, and on subsequent attempts to contact the device, the SP manager tries to use the default route and fails. If changing or deleting a private subnet, make sure to reassign all affected devices to another private subnet to avoid making devices unavailable.

To configure a private subnet:

1. Select the *Network - Private subnets* menu option.
2. Click the *Add Subnet* button. The Private Subnet configuration dialog appears.
3. Enter a meaningful name for the private subnet in the Private subnet name field.
4. Enter an IP address for the SP manager within the private subnet's network address range in the appliance side IP address field.
5. Enter a netmask for the private subnet in the Subnet netmask field.
6. Click *OK*.
7. Click *Save and apply changes*.

To configure a virtual network:

1. Select the *Network - Private subnets* menu option.
2. Under Virtual Network (DNAT) configuration, enter a virtual IP address to assign to the SP manager from the virtual network's address range in the Address field.
3. Enter the netmask for the virtual network in the Netmask field.
4. Click *Save and apply changes*.

Viewing Status Information about Active Sessions

By selecting the *Info - Active Sessions* menu option, the administrative user can view the status of active sessions.

Viewing System Information

By selecting the *Info - System information* menu option, the administrative user can view information about the system (such as kernel version, date and up time) and about the CPU.

Viewing Information about Detected Devices

By selecting the *Info - Detected devices* menu option, the administrative user can view information about detected devices.

Table 5.8: Information on the Info - Detected Devices Screen

Heading Name	Description
IP	IP address of the detected device.
MAC	MAC address of the detected device.
Configured as	Name/alias configured for the device on the SP manager.
DHCP Client?	If the SP manager's DHCP server is enabled and if the detected device obtained a dynamically allocated (instead of fixed) IP address from the SP manager, YES appears in this column. In all other cases, the column is empty.
DHCP Hostname	If a DHCP client sends a hostname as part of its DHCP request to the SP manager, and if the assigned address is not reserved, the DHCP hostname provided by the client appears in this column.
Port	The number of the SP manager private port through which the device is being detected.

NOTE: More than one device may be accessed through a single private Ethernet port; for that reason, configuration is done on devices not on ports. The Info - Detected devices screen is the only location in the Web Manager where the port to which a device is connected is identified.

Backing Up or Restoring Configuration Files

By selecting the *Mgmt - Backup/restore* menu option, the administrative user can configure backup and restoration of configuration files.

Clicking the *Save* button backs up the current state of the configuration files in a compressed file in Flash memory and overwrites any previous backup file.

Clicking the Load button overwrites the current state of the configuration files with the last backup copy that was made.

To back up configuration files:

1. Select the *Mgmt - Backup/restore* menu option.
2. Click the *Save* button to back up the current state of the configuration files.
3. Click *Save and apply changes.*

To restore backed-up configuration files:

1. Select the *Mgmt - Backup/restore* menu option.
2. Click the *Restore* button to restore any previously saved configuration files.
3. Click *Save and apply changes.*

Upgrading MergePoint 5224/5240 SP Manager Firmware

By selecting the *Mgmt - Firmware upgrade* menu option, the administrative user can upgrade the SP manager's operating system kernel and applications, which are collectively referred to as firmware in the management interfaces.

The current versions of the configuration files are used after the upgrade.

The upgraded software is used at the next boot, which should be performed after the upgrade completes.

The screen collects information used to automatically download software from an FTP server and to install the software on the SP manager.

Table 5.9: Firmware Upgrade Screen Fields

Field/Menu Name	Definition
FTP site	The DNS name or IP address of the FTP server where the firmware is located. You can use any ftp server if you download the firmware onto it first. The Cyclades ftp site address is: ftp.cyclades.com.
Username	Username recognized by the ftp server. The Cyclades ftp username for firmware downloads is "anonymous."
Password	Password associated with the username. An empty password is accepted for anonymous login at the Cyclades ftp server.
Image file (path and filename)	The pathname of the image file on the Cyclades ftp server. The directory pathname is in the form: /pub/cyclades/alterpath/onboard/released/V_<version_number>. The image filename begins with fl followed by a seven-digit number, as in fl2222222.bin. If needed, go to ftp://ftp.cyclades.com/pub/cyclades/alterpath/onboard/released in a browser to verify the correct pathname and file name for the software for the SP manager.

For more details about how images are stored in the SP manager and about configuration file backups, see Appendix D.

Special considerations for upgrading the firmware from a network boot

To upgrade using an image obtained from a network boot, boot the SP manager from a TFTP server before starting the upgrade procedure. Figure 5.5 shows the message that appears when the SP manager is running an image obtained from a network boot.

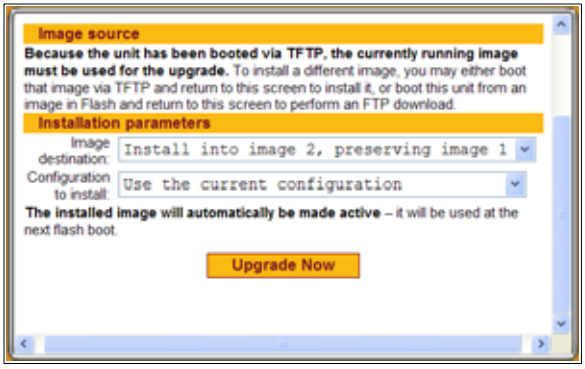
Image source
Because the unit has been booted via TFTP, the currently running image must be used for the upgrade. To install a different image, you may either boot that image via TFTP and return to this screen to install it, or boot this unit from an image in Flash and return to this screen to perform an FTP download.
Installation parameters
Image destination:
Install into image 2, preserving image 1
Configuration to install:
Use the current configuration
The installed image will automatically be made active – it will be used at the next flash boot.
Upgrade Now

Figure 5.5: Mgmt - Firmware Upgrade Screen With Net Boot Message

To download MergePoint 5224/5240 SP manager firmware:

1. Go to http://www.avocent.com.
2. Click *Support - Product* upgrades.
3. Follow the instructions on the page for accessing the firmware.

To upgrade the MergePoint 5224/5240 SP manager firmware:

1. To upgrade by saving a currently running image from the RAM memory into the Flash memory, boot from an image on a TFTP server following the network boot steps in *To configure boot:* on page 77. To upgrade with firmware from an ftp server, go directly to step 2.
2. Select the *Mgmt - Firmware upgrade* menu option.
3. To use the currently running image from the RAM memory into the Flash memory, perform the following steps:
   a. Select which boot image to overwrite from the Image destination pull-down menu.
   b. Choose a configuration option from the Configuration to install pull-down menu.
4. To upgrade using an image from an ftp server, perform the following steps:
   a. Enter the IP address or DNS name of the ftp server in the FTP site field.
   b. If desired, check the checkbox next to *Use passive mode FTP.*
   c. Enter the username for the ftp site in the Username field.
   d. Enter the password required for accessing the ftp site in the Password field.

e. Enter the pathname of the software image file on the ftp server in the Image file field.

5. Click the *Upgrade Now* button.
6. When the download completes, select the *Mgmt - Restart* menu option and restart the SP manager.

Restarting the MergePoint 5224/5240 SP Manager

By selecting the *Mgmt - Restart* menu option, the administrative user can reboot (restart) the SP manager.

To restart the MergePoint 5224/5240 SP Manager:

1. Select the *Mgmt - Restart* menu option.
2. Click the *Restart* button.

CHAPTER 6

Administration Tasks Not Performed in the Web Manager

This section lists the configuration and maintenance tasks that are performed by an administrator (either the root user, the admin user, or a member of the admin group) either on the Linux command line, using the cli utility or in the U-Boot monitor mode.

Configuring Storage of Buffered Data

If data buffering is enabled, console output from managed devices is sent to the syslog daemon but is not stored. This section describes how the root user can manually configure the storage of buffered data either in a directory mounted from an NFS file server or in a PC Flash memory card.

Table 6.1: Configuration Files Used in Data Buffering

File	Use
/etc/fstab	If using an NFS-mounted directory for storage, modify the /etc/fstab file to define the NFS mount point. **NOTE:** This file does not need to be edited for mounting a compact Flash PC card, because a compact Flash card is detected and automatically mounted under the /mnt directory when the appliance is rebooted after card installation.
/etc/syslog-ng/syslog-ng.conf	Device data received by the appliance is sent to the syslog-ng daemon, which uses this file. This file can be modified to configure buffered data from all devices to be stored in a single file. See *To store buffered data in multiple files, one for each target device:* on page 112.
/usr/sbin/cyc-conserver	Determines what is inserted into the conserver.cf file when a new device is added. This file can be modified to configure buffered data from each device to be stored in a separate file. See *To store buffered data in multiple files, one for each target device:* on page 112. **NOTE:** The /usr/sbin/ directory is mounted read-only by default. The procedure describes how you can mount the /usr/sbin/ directory in read-write mode before you can edit the cyc-conserver file.
/etc/conserver.cf	Determines where data buffer files are stored. Direct user modifications to conserver.cf are lost whenever a new device is added, so make any desired changes to the cyc.conserver file instead.

To store buffered data in a single file:

1. Log into the appliance's console as root.
2. Add the following entries to the syslog-ng.conf file.

   The example entries configure data buffer storage in an NFS-mounted /mnt/nfs_server/log/device.log file.

   ```
   source src_dev_log { unix-stream("/dev/log"); };
   filter f_device { program("conserver");};
   destination d_device { file("/mnt/nfs_server/log/device.log"); };
   log { source(src_dev_log); filter(f_device); destination(d_device); };
   ```

3. Put the syslog-ng.conf file changes into effect by stopping and restarting syslog-ng, as shown in the following command line.

   ```
   $ killall -hup syslog-ng
   ```

   The configuration changes are saved to the SP manager's resident Flash memory if the SP manager is booted from a local image.

To store buffered data in multiple files, one for each target device:

1. Log into the appliance's console as root.
2. Use the **cat** command to display the contents of the /proc/cmdline file to see which boot image is currently running.

   ```
   [root@MergePoint5224 /]# cat /proc/cmdline
   root=/dev/hda6 console=ttyS0,9600
   ```

   If the output shows root=/dev/hda5, Image 1 is running, and if root=/dev/hda6, Image 2 is running.

3. Mount the directory for the running image with read-write permission.

   ```
   $ mount -t ext2 -o rw,remount /dev/hda5
   ```

   -or-

   ```
   $ mount -t ext2 -o rw,remount /dev/hda6
   ```

4. Open the /usr/sbin/cyc-conserver file for editing.

   ```
   $ cd /usr/sbin
   $ vi cyc-conserver
   ```

5. Change the variable LOGDIR to the pathname of the directory where you want the data buffer files to be stored.

   ```
   'LOGDIR=/mnt/nfs_server/log'
   ```

   -or-

```
'LOGDIR=/mnt/pc_compact_flash_card/log'
```

6. Remove the following line.

```
llset('conserver', "server/$server/logfile", "/dev/null"),
```

7. Ensure the following line is still present or enter it in place of the deleted line above:

```
llset('conserver', "server/$server/logfile", "$server.log"),
```

NOTE: This example configuration stores the buffered data in separate files according to each device's alias. Adding devices automatically results in their data being buffered to a device-specific logfile.

Using MindTerm to Create an SSH Tunnel

This section describes how an administrative user can create an SSH tunnel from a user's workstation to a managed device using the MindTerm applet that activates when any user connects to the console using the Web Manager. A regular user cannot use this procedure because regular users who connect to the console are restricted to selecting options from a limited-access menu, and the Tunnels option is not available for them on the MindTerm menu.

To use MindTerm to create an SSH tunnel:

1. Log into the Web Manager as an administrative user, and select the *Access - Appliance* menu option. A window running a MindTerm applet appears, with an encrypted SSH connection between the user's computer and the console.
2. Log in and follow any prompts that may appear about saving the host key.
3. Press **Ctrl** and the right mouse button at the same time (**Ctrl**+[mouse right-click]) then drag the cursor to pull down and select the *Tunnels - Basic* menu option.

   The MindTerm Basic Tunnels Setup dialog box appears.

4. Enter a TCP port number to forward in the Local port field. You can select a random number over 1000.
5. Enter the device's port number to bring up the desired web application in the Remote port field.
6. Enter the IP address of the device in the Remote Host field.
7. Click *Add*.

   The tunnel is created and the dialog box appears similar to the following screen example.

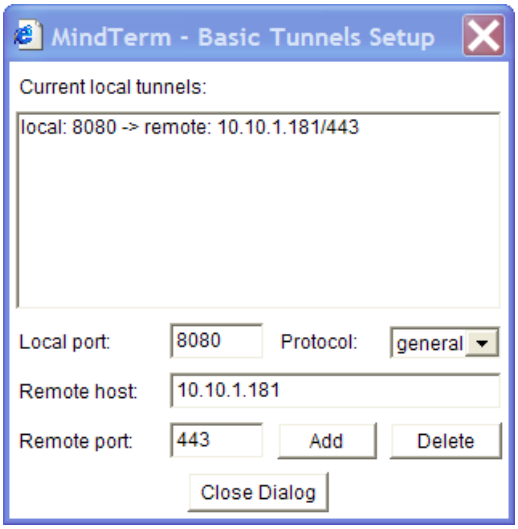

Figure 6.1: MindTerm Basic Tunnels Setup Dialog Box

Specifying the Location for the OTP Databases

As configured on the SP manager, OTP expects its user databases to reside in /mnt/opie/etc. The SP manager's resident Flash memory does not provide a directory for the OTP databases. Administrator must mount a device on /mnt/opie. You may use a compact Flash PC card or an NFS-mounted directory.

To configure a compact Flash card for OTP, the root user logs into the console and runs the /bin/do_create_cf_ext2 script on the command line. The script does the following:

- Creates a partition on the compact Flash (sfdisk /dev/hdc)
- Creates an ext-2 filesystem on the compact Flash (mke2fs /dev/hdc1)
- Mounts the compact Flash on the /mnt/opie directory (mount -t ext2 /dev/hdc1 /mnt/opie/)
- Creates the directory /mnt/opie/etc
- Creates the file /mnt/opie/etc/opiekeys
- Sets the permissions of the file to mode 0644, the owner of file to root and the group to bin
- Creates the directory /mnt/opie/etc/opielocks for the OPIE lock files
- Sets the permissions of this directory to 0700 and the owner and group to root

To configure a PC compact Flash card for OTP database storage:

1. Log into the console as root.
2. Enter the **/bin/do_create_cf_ext2** script on the command line.

To configure a NFS-mounted directory for OTP database storage:

1. Make sure a directory (for example /home/opie), has been created on the NFS server and is shared (exported) via NFS.
2. Log into the console as root.
3. Enable the RPC service using the **cli** utility.

   ```
   [root@MergePoint5224 /]# cli -CF set service rpc enable yes
   ```

4. Mount the directory from the NFS server.

   The following screen example uses nfs_server.avocent.com as the NFS server name and /home/opie as the exported directory's name.

   ```
   [root@MergePoint5224 /]# mount -t nfs nfs_server.avocent.com:\
   /home/opie /mnt/opie
   ```

5. Enter the following commands to create the /etc directory on the mounted directory and to create an opiekeys file.

   ```
   [root@MergePoint5224 /]# mkdir /mnt/opie/etc
   [root@MergePoint5224 /]# touch /mnt/opie/etc/opiekeys
   [root@MergePoint5224 /]# chmod 0644 /mnt/opie/etc/opiekeys
   [root@MergePoint5224 /]# chown root:bin /mnt/opie/etc/opiekeys
   ```

To configure OTP authentication for modem or GSM phone card dial-ins:

1. Log into the console as root.
2. Use **vi** or another text editor to open the /etc/mgetty.login.config file for editing and find this entry: * - - /bin/login.

   ```
   [root@MergePoint5224 /]# vi /etc/mgetty.login.config
   ...
   *       -       -       /bin/login @
   ```

3. Replace login with opielogin.

   ```
   *       -       -       /bin/opielogin @
   ```

4. Save and quit the file.

To configure OTP authentication for SSH or console logins:

This procedure manually configures Telnet or SSH logins to the console with either the OTP or OTP/Local authentication method, and it also changes the targets of the symbolic links /etc/pam.d/sshd and /etc/pam.d/login to /etc/pam.d/[otp,otplocal].

NOTE: The Web Manager does not support OTP authentication.

1. Change to the /etc/pam.d directory.

   ```
   [root@MergePoint5224 /]# cd /etc/pam.d
   ```

2. To specify OTP for logins to the console or through telnet, change the target of the symbolic link login to otp or otplocal.

CAUTION: If OTP is chosen, users (even root) may be locked out if not configured properly. You can test whether OTP is working by first changing only the symbolic link for login as shown in the following screen example and then attempting access using telnet. If the telnet login using an OTP password succeeds, you can safely change the method for ssh logins as described in step 3.

```
[root@MergePoint5224 /]# ln -sf /etc/pam.d/otp login
```

-or-

```
[root@MergePoint5224 /]# ln -sf /etc/pam.d/otplocal login
```

3. To specify OTP for ssh logins, change the target of the symbolic link sshd to otp or otplocal.

   ```
   [root@MergePoint5224 /]# ln -sf /etc/pam.d/otp sshd
   ```

   -or-

   ```
   [root@MergePoint5224 /]# ln -sf /etc/pam.d/otplocal sshd
   ```

NOTE: The cli utility and the Web Manager may not display the correct authentication information when the symbolic links are changed manually.

To configure OTP authentication for a device:

This procedure manually configures a previously configured device or devices to use the OTP or OTP/Local authentication method.

1. Log into the appliance's console as root.
2. Open the /etc/onboard_server.ini file for editing.
3. For any configured device, set the authtype to be either otp or otplocal.

   ```
   authtype = otp
   ```

   -or-

   ```
   authtype = otplocal
   ```

4. Save and quit the file.

How Users are Registered with OTP and Obtain OTP Passwords

All users who need to use OTP authentication must have a local account on the SP manager, must be registered with the OTP system and must be able to obtain OTP passwords.

The OPIE commands in the following bulleted list must be executed with the -c option while the user is logged in locally through the console port:

- The opiepasswd command
- The opiekey command to generate OTP passwords

The requirement for local logins through the console port is enforced for regular users because running the commands through a dial-in or other unsecure connection may expose the user passwords, pass phrases and OTP passwords. The root user can execute these commands without the -c option while logged in over ssh because ssh provides a secure path. These commands should never be executed over a dial-in or Telnet connection:

OTP passwords are generated in one of the two following ways:

- By the user or administrator executing the opiekey command: If opiekey command is executed by an administrator on behalf of a user, the administrator must give the OTP username and the user's secret pass phrase to each user along with the generated OTP passwords.
- By the user with a password generating device: If a user has a password generating device, then the user generates the OTP password when challenged at login using the username and secret pass phrase, along with the seed and sequence number that are displayed along with the OTP challenge.

To register and generate OTP passwords for users:

The following procedure shows an example of an administrator logging in locally through the console port, registering a user and generating OTP passwords for the user. The example shows using cli to add the user, but any of the tools available for adding users, including the Web Manager, may be used to configure the user account beforehand.

1. Log into the appliance console as root.
2. Make sure each user authorized for dial-ins has a local account on the SP manager.

   If using the cli utility to add the user, perform the following steps:

   a. Add the user and set the user's password.

      The following screen example shows using the **cli** utility to add user joe and set the user's password to joes_passwd.

      ```
      [root@MergePoint5224 /]# cli
      cli> add user joe
      OK
      cli> set user joe passwd joes_passwd
      OK
      ```

   b. If the user must access devices through the SP manager, add the user as a spmanager user.

NOTE: Adding users through the Web Manager adds them as normal UNIX users and as spmanager users without requiring a separate step.

```
cli> add spmanager user joe
OK
```

c. If you are using cli, commit the changes.

```
cli> commit
OK
cli> exit
[root@MergePoint5224 /]#
```

3. Enter the **opiepasswd** command to register the user.

   The following example shows using opiepasswd with the -c option while logged in locally through the console port. If you are logged into the console using ssh, do not use the -c option. The example uses joe as the username and joes secret pass phrase as the secret pass phrase.

NOTE: The secret pass phrase is not the same as the user's regular login password.

In the example, the opiepasswd command generates a default OPIE sequence number of 499 and a creates a seed (or key) from the first two letters of the hostname and a pseudo random number, in the example on93564.

```
[root@MergePoint5224 /]# opiepasswd -c joe
Adding joe
Reminder - Only use this method from the console; NEVER from remote. If
you are using telnet, xterm, or a dial-in, type ^C now or exit with no
password. Then run opiepasswd without the -c parameter. Using MD5 to
compute responses.
Enter new secret pass phrase: joes secret pass phrase
Again new secret pass phrase: joes secret pass phrase

ID joe OPIE key is 499 on93564
CITY MARY GLOW BIll MAY ARM
[root@MergePoint5224 /]#
```

4. If desired, enter **opiekey** to generate a number of passwords for the user.
5. Give the OTP username, secret pass phrase and any OTP passwords generated in this procedure to the user.
6. Save the changes by entering the **saveconf** command.

Replacing the Self-Signed Certificate With an SSL Certificate for HTTPS

As described in *HTTPS on the MergePoint 5224/5240 SP Manager* on page 28, an administrator must replace the automatically generated self signed certificate with an SSL certificate from an official certificate authority. The root user can follow the instructions in the following procedure to generate a certificate signing request; after obtaining the certificate from the CA, the root user then must install the public key and the certificate in the Apache web server on the SP manager.

To replace the self-signed certificate with one from a certificate authority:

1. Log into the console as root.
2. Use **openssl** with the req parameter to create a private key and a public CSR (certificate signing request).

   Use the command line shown in the following screen example.

   ```
   [root@MergePoint5224 /]# openssl req -new -nodes -keyout private.key \
   -out public.csr
   ```

   The utility prompts for information. The required information is shown in the following table. Any other requested information is not required.

Table 6.2: Required Information When Creating an SSL Certificate Request

Prompt	What You Enter
Country Name (2 letter code) [AU]:	The country code consisting of two letters
State or Province Name (full name) [SomeState]:	The full name (not the postal abbreviation) of the state
Locality Name (e.g., city) []:	The name of your city
Organization Name (e.g., company) [Internet Widgits Ltd]:	The organization for which you want to obtain the certificate
Organizational Unit Name (e.g., section) []:	The department or section
Common Name (e.g., your name or your server's hostname) []:	The name of the machine where the certificate must be installed
Email Address []:	Your email address or the administrator's email address

   The generated request automatically includes the public key.

3. Submit the CSR request to the certificate authority (CA).

   After receiving the certificate from the CA, perform the remaining steps:

4. Copy the private key into /etc/httpd/conf/ssl.key/server.key.

```
[root@MergePoint5224 /] cat private.key-/etc/httpd/conf/ssl.key/
server.key
```

5. Copy the certificate into /etc/httpd/conf/ssl.crt/server.crt.

   The following screen example uses cert.crt as the name of the certificate file from the CA. Substitute the correct name for your file.

```
[root@MergePoint5224 /] cat cert.cert-/etc/httpd/conf/ssl.crt/
server.crt
```

NOTE: By default, the /etc/httpd/conf/ssl.key/server.key and /etc/httpd/conf/ssl.crt/server.crt files are listed in /etc/config_files so they can be automatically saved in the Flash memory whenever the saveconf command is run or the administrative user saves the configuration files using the Save button on the Mgmt - Backup/restore screen.

6. Run the **saveconf** command to save the configuration in Flash.
7. Restart the web server to put the certificate into effect.

```
[root@MergePoint5224 /] daemon.sh restart APACHE
```

Configuring the DHCP Server

To enable DHCP to configure IP address for target devices, the administrator must perform DHCP configuration manually. The root user logs into the appliance's command line and performs the following steps.

- Enables the dhcpd by editing /etc/dhcpd.sh.
- Makes the appropriate configuration changes and specifies fixed addresses for all devices in the /etc/dhcpd.conf file.
- Saves the configuration file changes in the firmware using the saveconf command.
- Reboots or restarts the dhcpd service manually.

To configure DHCP for managing IP addresses of target devices:

1. Log into the console as root.
2. Open the /etc/dhcpd.conf file for editing.
3. Copy and paste the sample configuration section.
4. Remove the comment (#) signs at the beginning of the lines in the pasted section.

```
#  ######## SAMPLE CONFIGURATION ###############
subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.110 192.168.0.119;
        default-lease-time 86400;
        max-lease-time 172800;
        option broadcast-address 192.168.0.255;
```

```
        option routers 192.168.0.10;
        option subnet-mask 255.255.255.0;
        option domain-name-servers 192.168.0.11;
        option domain-name “cyclades.com.au”;
        host MySP {
                hardware ethernet 00:e0:4c:ec:12:26;
                fixed-address 192.168.0.211;
       }
#  ##############################################
```

5. Configure a hostname and fixed address for each device by performing the following steps.
   a. Find the host MySP line and replace MySP with a hostname/alias for the device.
   b. Specify the MAC address of the device on the line that begins hardware ethernet.
   c. Specify the desired IP address for the device on the line that begins fixed-address.

      For example, see the following edited host entry.

```
host sp1 {
        hardware ethernet 00:60:2e:bb:aa:aa;
        fixed-address 192.168.0.21;
}
```

   d. Copy and paste the three lines that define the IP address for a device as many times as needed and then make the edits to specify the desired IP address for each device.
6. Make other changes as appropriate for your environment, removing the comment (#) signs at the beginning of all edited lines.
7. Save and quit the file.
8. Open the /etc/dhcpd.sh file for editing.

```
# This file defines the dhcpd service configuration

ENABLE=NO                   # Must be "NO" or "YES" (uppercase)
DNAME=dhcpd                 # daemon name
DPATH=/usr/sbin             # daemon path
ShellInit=                  # Performs any required initialization
ConfigFiles=/etc/dhcpd.conf # configuration files
DTYPE=sig                   # must be "sig" or "cmd"
DSIG=kill         # signal to stop/restart the daemon (lowercase)
```

```
                    # if it's hup term will be used to stop the daemon
# daemon command line parameters
DPARM="-q priv0"
DSTOP=
```

9. Change the definition ENABLE=NO to ENABLE=**YES**.

   ```
   ENABLE=YES # Must be "NO" or "YES"(uppercase)
   ```

10. Save and quit the file.
11. Save the configuration file changes by entering the **saveconf** command.
12. Start dhcpd by either restarting the SP manager or restarting dhcpd.

    The following screen example shows the syntax for restarting dhcpd.

    ```
    [root@MergePoint5224 /]# daemon.sh restart DHCPD
    ```

Configuring Dial-ins Using cli

The following procedures give examples for configuring the two following types of devices for dial-ins.

- An external modem connected to an AUX port
- A modem, GSM or CDMA PC card installed in one of the front card slots. Configure the card in slot 1 as modem0 and configure the card in slot 2 as modem1

See Table 4.13 on page 42 for the values you need to configure for each access type.

To configure an external modem or a modem, GSM or CDMA PC card using cli:

NOTE: Where cli commands set parameters for PCMCIA modem or phone cards, the cardtype is either modem0, modem1, gsm0 or gsm1.

1. Log into the console as root.
2. Enter the **cli** command.
3. If you are configuring an external modem, set the **auxport profile** to **modem**.

   ```
   cli> set auxport profile modem OK
   ```

4. Set the access **type** to **autoppp**, **login**, **ppp** or **otplogin**.

   The following example sets the access type of an external modem to ppp.

   ```
   cli> set auxport modem type ppp
   OK
   ```

The following example sets the access type of modem PC card modem0 to ppp.

```
cli> set cards modem0 autoppp
OK
```

5. Set or accept the default **speed**.

   The default speed is 9600. The following example sets the external modem speed to 4800.

   ```
   cli> set auxport modem speed 4800
   OK
   ```

   The following example sets the speed of modem PC card modem0 to 4800.

   ```
   cli> set cards modem0 speed 4800
   OK
   ```

6. Set or accept the default flow control (**data-flow**).

   The following example sets an external modem's data-flow type to both.

   ```
   cli> set auxport modem data-flow both
   OK
   ```

   The following example sets the data-flow type of modem PC card modem0 to both.

   ```
   cli> set cards modem0 data-flow both
   OK
   ```

7. Set the chat initialization AT commands (**initchat**).

   Put quotation marks before and after the chat string and put backslashes (\) before any quotation marks or backslashes that are part of the chat string. The examples set the chat string to: initchat " " " ATZ OK.

   The following example sets an external modem's chat string.

   ```
   cli> set auxport modem initchat "\"\" ATZ OK"
   ```

   The following example sets the chat string of modem PC card modem0.

   ```
   cli> set cards modem0 initchat "\"\" ATZ OK"
   OK
   ```

8. If you set the access type to ppp or autoppp, set all ppp parameters by performing the following steps.

a. Enable authentication as a requirement for PPP connections, if desired, by using the **auth** parameter followed by **yes**.

The following example enables authentication for an external modem.

```
cli> set auxport modem ppp auth yes
OK
```

The following example enables authentication for modem PC card modem0.

```
cli> set cards modem0 ppp auth yes
OK
```

b. Accept the default local IP address or set another by using the **iplocal** parameter.

The following example configures a local IP address for an external modem.

```
cli> set auxport modem ppp iplocal local_IPaddress
OK
```

The following example configures a local IP address for modem PC card modem0.

```
cli> set cards modem0 ppp iplocal local_IPaddress
OK
```

c. Accept the default remote IP address or set another by using the **ipremote** parameter.

The following example configures a remote IP address for an external modem.

```
cli> set auxport modem ppp ipremote remote_IPaddress
OK
```

The following example configures a remote IP address for a modem PC card modem0.

```
cli> set cards modem0 ppp ipremote remote_IPaddress
OK
```

9. Accept the default maximum transmission unit or set another by using the **mtu** parameter.

The following example sets the MTU to 1200 for an external modem.

```
cli> set auxport modem ppp mtu 1200
OK
```

The following example sets the MTU to 1200 for modem PC card modem0.

```
cli> set cards modem0 ppp mtu 1200
OK
```

10. Accept the default maximum receive unit or set another value by using the **mru** parameter.

    The following example sets the MRU to 1200 for an external modem.

    ```
    cli> set auxport modem ppp mru 1200
    OK
    ```

    The following example sets the MRU to 1200 for modem PC card modem0.

    ```
    cli> set cards modem0 ppp mru 1200
    OK
    ```

11. Accept the default PPP options or set others by using the **options** parameter followed by the desired options in quotes.

    The following example sets the ppp options for an external modem.

    ```
    cli> set auxport modem ppp options "options"
    OK
    ```

    The following example sets the ppp options for modem PC card modem0.

    ```
    cli> set cards modem0 ppp options "options"
    OK
    ```

12. If configuring a GSM card, set a **pin** number.

    The following example sets a pin number 22222 for phone PC card gsm0.

    ```
    cli> set cards gsm0 pin 22222
    OK
    ```

13. Commit the changes and quit.

    ```
    cli> commit
    OK
    cli> quit
    ```

Configuring the Users' Console Login Menu

Regular users are configured with /usr/bin/rmenush as their default login shell. All users with rmenush as their login shell see the same menu whenever they log into the console.

The SP manager administrator can configure the rmenush menu to display other options including links to additional submenus or commands by modifying the /etc/menu.ini file.

CAUTION: If changing the default menu, the administrator must ensure that any added programs do not introduce security vulnerabilities.

The administrator must know the following about the behavior of rmenush before configuring any changes to the menu:

- If the called program exits with a return code indicating an error, rmenush prompts the user to press any key to continue.
- Any error messages generated by the called program are left on the screen for the user to read. Examples showing how the administrator can force this behavior on for successful programs and off for unsuccessful ones are provided in the configuration file.
- The SP manager administrator assigns the /usr/bin/rmenush shell to users as appropriate, by editing the /etc/passwd file entries for the users.

When editing the menu.ini file, the administrator must know the following:

- Spaces are shown in menu items by the use of an underscore between words.
- An underscore cannot be displayed in the menu text.
- The right-hand value of each name/command pair is assumed to be either a menu defined in the menu.ini file or a command.
- A maximum of 16 menu items can display on the screen at a time. Any extra menu items can be reached by using the arrow keys to scroll down.

To modify the user shell menu:

See *Configuring the Users' Console Login Menu* on page 126 for background information and examples.

CAUTION: If adding programs to the menu, take care the commands do not allow the user to break out of the programs they call.

1. Log into the appliance console as root.
2. Open the /etc/menu.ini file for editing.
3. Add new menus and menu items as desired, using underscores (_) to indicate spaces between words.
    a. In the [main] menu definition, insert a definition for an action or an option for a submenu, as desired.

The following example shows a new menu option with a command defined along with a link to a new subnet identified with the newsubmenu keyword.

```
[main]
    Access_Servers = /bin/spshell
    Change_Password = /usr/bin/passwd
    New_Menu_Option = command_pathname_and_options
    New_Submenu = newsubmenu
```

b. Add a definition for a submenu using the defined keyword.

```
[newsubmenu]
    Submenu_Option1 = command_pathname_and_options
    Submenu_Option2 = command_pathname_and_options
```

4. Save and quit the file.

Configuring Routes With cli

The following procedures give examples for using the cli utility for configuring default, host and network routes and assigning them to interfaces or to gateways.

NOTE: Setting a gateway IP address automatically creates a default route to the gateway's IP address.

To configure routes with cli:

1. Log into the console as root.
2. Enter the **cli** command.
3. Make sure the interface for which you want to configure a route is active.

```
cli> set network interface interface_name active
yes

OK
```

4. Set a default route by setting a gateway IP address.

```
cli> set network interface interface_name gateway gatewayIP

OK
```

5. Add a host route, if desired, by entering the host's IP address after the add network st_routes command.

```
cli> add network st_routes hostIP
```

6. Add a network route, if desired, by entering the network address after the add network st_routes command in the form 1.2.3.4/24.

```
cli> add network st_routes networkIP/24
OK
```

7. For both host and network routes, use the set network st_routes command to assign the route to an interface or to a gateway and optionally assign it a metric, by performing the following steps.
   a. To assign the route to an interface, enter set network st_routes IPaddress | networkIPaddress/NN device ethN.

      The following screen example shows assigning the host route created in step 5 to the device eth0 and assigning an optional metric.

```
cli> set network st_routes IPaddress | networkIPaddress/NN ethN \
metric N
OK
```

   b. To assign the route to a gateway, enter set network st_routes IPaddress | networkIPaddress/NN gateway gatewayIP.

      The following screen example shows assigning the network route created in step 6 to the gateway 192.168.2.0.

```
cli> set network st_routes IPaddress | networkIPaddress/NN \
gateway gatewayIP
OK
```

Saving Configuration Changes

As described in *How Configuration Changes Are Handled* on page 55, the Web Manager and the cli utility do not save changes as they are made. The following procedures show the steps administrators need to take to save changes to configuration files in different environments on the SP manager.

When changes are made by an administrative user using the Web Manager, an Unsaved changes button displays until the administrative user clicks the *Save and apply changes* button.

When changes made by the administrator using the cli utility are not saved (committed) and the administrator enters the quit command, the utility displays the prompts shown in the following screen example.

```
cli> quit
You have made changes but haven't committed them yet.
To commit the changes, use the "commit" command.
To revert all changes and quit without committing, use "quit!".
```

To save configuration changes:

1. If you are logged into the Web Manager as an administrative user, click *Save and apply changes*.
2. To save configuration changes made while using the cli utility, either invoke the **cli** utility using the **-C** option or enter the **commit** command after performing configuration and before quitting cli.

Backing Up Configuration Files

SP manager administrators can create a compressed backup of all configuration files and store the backup in /mnt/hda3/backup/configuration_files.gz. Any compressed configuration file that already resides in the directory is overwritten. The following procedures show how administrators can back up configuration files in different environments on the SP manager.

To back up configuration files:

1. If you are logged into the Web Manager as an administrative user, go to the Mgmt - Backup/restore screen and click the *Save* button.
2. If you are logged into the console as root, enter the **saveconf** command.

```
[root@MergePoint5224 /root]# saveconf
```

Restoring Backed Up Configuration Files

This procedure assumes that you or a previous administrator has previously either run the saveconf command or clicked the Save button on the Web Manager Mgmt - Backup/restore screen after making changes to the configuration. This procedure restores the configuration files to the state they were in when they were last backed up.

To restore the configuration files to the last saved version:

1. If you are logged into the Web Manager as an administrative user, click the *Load* button on the Web Manager Mgmt - Backup/restore screen.

2. If you are logged into the console as root, enter the **restoreconf** command.

```
[[root@MergePoint5224 /root]# restoreconf
```

Restoring Factory Default Configuration Files

A root user can restore the factory default configuration files from the factory_default_files.gz file by performing the following procedure while logged in through the console, via telnet or ssh to restore the configuration files to the state they were in when the SP manager shipped. For how to restore factory defaults while you are saving a boot image from RAM memory onto the resident Flash memory, see *To upgrade to a boot image from a network boot:* on page 204.

To restore the factory default configuration files from the command line:

1. Log into the console as root.
2. Enter the **restoreconf** command with the factory_default option.

```
[root@MergePoint5224 /root]# restoreconf factory_default
```

Adding New Files to Be Backed Up and Restored

The /etc/config_files file lists all files to be backed-up and restored, including its own filename.

If you add an application or a script or a data file to the system, make sure to add the file's pathname to the config_files file.

To configure an added script or other file for backup and restoration:

1. Log into the console as root.
2. Change to the /etc directory.

```
[root@MergePoint5224 /]# cd /etc
```

3. Open the config_files file for editing.

```
[root@MergePoint5224 /]# vi config_files
```

4. Add the pathname of the new file to the list.

```
/etc/ypbind.conf
/etc/yp.conf
/etc/localtime
/etc/timezone
/pathname/to/new/file
```

5. Save and quit the file.

Changing Web Manager Time-outs

The root user can log into the console as root and manually specify a time-out value for Web Manager sessions. The expiration of a Web Manager session after a period of inactivity may be configured using the cli utility along with either or both of two time-out-related parameters that have different effects. Their values can be set to any number of seconds up to 2e31.

Table 6.3: Web Manager Time-out-related cli Parameters

cli parameter	Description
browser_timeout	Default: no setting. When set, if the specified period of inactivity occurs while a user is logged into the Web Manager, the user is automatically logged out of the Web Manager. Any DirectCommand sessions are automatically terminated. To set a time-out value that does not automatically terminate DirectCommand sessions when the number of seconds of inactivity elapses, set session _timeout.
session_timeout	Default: no setting. Causes the user's session to expire if the specified period of inactivity occurs but does not log the user out unless the user clicks any of the Web Manager controls. Preventing user activity without automatic logouts allows DirectCommand sessions to continue.

Table 6.4: Examples of Web Manager Time-out-related cli Parameter Settings

With these settings . . .	These effects occur . . .
session_timout=900 (15 minutes) browser_timeout= (not set)	After 15 minutes, the user's session is automatically terminated, and the user is logged out.
session_timout=900 (15 minutes) browser_timeout=7200 (120 minutes)	After 15 minutes and before 120 minutes of inactivity, the user's session is automatically terminated, but the user is not logged out unless the user clicks any of the Web Manager controls. After 120 minutes of inactivity, the user is automatically logged out. Between 15 minutes and 120 minutes, if the user does not click any controls, DirectCommand sessions can continue.

To configure Web Manager time-outs:

1. Log into the console as the root user.

```
MergePoint5224 login: root
Password: password
```

2. Enter the **cli** command. The cli> prompt appears.

```
[root@MergePoint5224 /root]# cli
```

3. If desired, set the browser_timeout value.

```
cli> set web browser_timeout <seconds>
```

4. If desired, set the session_timeout value.

```
cli> set web session_timeout <seconds>
```

5. Save the changes.

```
cli> commit
```

6. Exit from the cli utility.

```
cli> quit
```

Changing the Sort Order of Device Listings

The names of devices are listed in the Web Manager and by spshell in the order in which they were configured. An administrator can configure device lists to appear in alphabetical order using the cli utility.

To sort the device list alphabetically:

1. Log into the console as an administrative or root user.

```
MergePoint5224 login: root
Password: password
```

2. Enter the **cli** command.

```
[root@MergePoint5224 /root]# cli
```

3. Set the sort order by entering the spmanager global sort server alpha parameters.

```
cli> set spmanager global sort server alpha
```

4. Save the changes.

```
cli> commit
```

5. Exit from the cli utility.

```
cli> quit
```

6. Log out and bring up the Web Manager Config - Devices screen. The devices now display sorted alphabetically by name.

Configuring Groups for Use with Authentication Servers

This information applies when an authentication method that relies on an authentication server is configured either for the SP manager or for a target device. If the administrator of an authentication server configures users as members of groups as described in this section, the users do not need to have accounts configured on the SP manager.

For example, if user johnb is defined as a member of the admin group on a TACACS+ server, johnb can log into the SP manager as an administrative user when TACACS+ authentication is configured for the SP manager, even though no user account is configured for johnb on the SP manager.

To support the use of groups with the authentication methods that support groups, the administrator must configure local groups on the SP manager using the same group names used on the authentication servers, using the Web Manager or the cli utility.

The admin group exists by default. User accounts do not need to be configured on the SP manager for the users in the authentication-server-defined groups.

Configuring group authorization for LDAP authentication

Group authorizations can be provided by either a Windows Active Directory (AD) server or a server running OpenLDAP:

- On an AD server, the info attribute can be used to define groups, but the memberOf attribute is already used in the AD schema to denote domain membership and so it cannot be used to defining groups.
- On an OpenLDAP server, either the info attribute or memberof attribute can be used.

Configuring group authorizations on an AD server

Perform the following procedures for configuring support for group authorizations when a Windows Active Directory server is used for LDAP authentication.

To install Windows Administration Pack tools and configure the snap-in:

1. On the server, install the tools from the Windows Administration Pack. The tools are found on the Windows server installation CD.
2. Go to the start menu and click *Run*.
3. In the Open field, type **mmc /a** and click *OK*. A console window appears.
4. Click *Console* in the console window menu bar and select *Add/Remove Snap-in...*. The Add/Remove Snap-in window appears.
5. Click *Add*. The Add Standalone Snap-ins window appears.
6. Select *Active Directory Schema* from the list of snap-ins and click *Add*.
7. Select *ADSI Edit* from the list of snap-ins and click *Add*.
8. Click *Close*.

9. Click *OK* in the Add/Remove Snap-in... window.

To configure Active Directory schema:

1. In the server's console window, double-click *Active Directory Schema*. The paths Classes and Attributes appear.
2. Double-click *Attributes* and confirm that the info attribute is present.
3. Double-click *Classes*, locate the class Users and right-click to select *Properties*.
4. Select the *Attributes* tab and click *Add*.
5. Locate info in the attributes list; click *Apply* and then *OK*

To configure a group in ADSI Edit:

1. In the server's console window, double-click *ADSI Edit*.
2. From the menu, select *Action - Connect to...*. The Connection window appears.
3. Accept the defaults and select *OK*.

   The path Domain NC<*domain*>.com appears.
4. Double-click *Domain NC<domain>.com*. The expanded path DC=XXX,DC=*XXX*,DC=com appears.
5. Double-click *DC=xxx,DC=xxx,DC=com*.

   The expanded class CN=Builtin, ... appears.
6. Double-click *CN=Users*. The expanded users list appears.
7. Right-click on the name of a user and select *Properties*. The CN=<username> Properties window appears.
8. In the Optional area under Select which property to view: locate and select *[info]*.
9. In the Edit Attribute field, enter the group name in the format group_name=<Group1>. If the username selected is an administrative user, enter admin as the group_name.
10. Click *OK*.
11. Close or save the windows.

Defining groups on an LDAP server running OpenLDAP

Perform the following procedures for configuring support for group authorizations when a server running OpenLDAP is used for LDAP authentication.

Any groups configured in the memberof attribute are used; if no groups are defined in the memberof attribute, then any groups configured in the info attribute are used. The groups defined on the LDAP server must be configured on the SP manager with the desired device access authorizations.

To configure groups using the info attribute on an LDAP authentication server:

1. On the server, add the info attribute into the objectclass posixAccount in the /etc/ldap/schema/nis.schema file.

   ```
   objectclass (1.3.6.1.1.2.0 NAME 'posixAccount' SUP top AUXILIARY DESC
   'Abstraction of an account with POSIX attributes' MUST ( cn $ uid $
   uidNumber $ gidNumber $ homeDirectory ) MAY ( userPassword $ loginShell
   $ gecos $ description $ info) )
   ```

2. Make sure the info attribute exists in the /etc/ldap/schema/cosine.schema file.

   ```
   attributetype (0.9.2342.19200300.100.1.4 NAME 'info'
   DESC 'RFC1274: general information'
   EQUALITY caseIgnoreMatch
   SUBSTR caseIgnoreSubstringsMatch
   SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{2048} )
   ```

3. Make sure both schema files are listed in slapd.conf:

NOTE: The slapd.conf file is normally located in: [Redhat] /etc/openldap or [bsd] /usr/local/etc/openldap.

   ```
   include /etc/openldap/schema/nis.schema
   include /etc/openldap/schema/cosine.schema
   ```

4. Restart the LDAP service to activate changes.
5. Use the **ldapadd(1)** command to add new users or the **ldapmodify(1)**command to assign a user to one or more groups in one of the two following ways:
   a. Enter the user information including the group name or names on the command line, using the **ldapadd** command to add new users or the **ldapmodify** command to modify existing users.
   b. Put all user information, including the group definition in a text file and use the text file with the -f option on the command line to configure groups for users.

      Use the following syntax for configuring a group using the info attribute:

      ```
      info: group_name=<Group1>[,<Group2>,...,<GroupN>];
      ```

NOTE: To give a user administrative access to the MergePoint 5224/5240 appliance, add the admin group name to the group_name definition.

To configure groups using the memberof attribute on an LDAP authentication server:

1. On the server, add the memberof attribute to the /etc/openldap/schema/core.schema file.

   ```
   attributetype (1.2.840.113556.1.2.102 NAME 'memberof'
   DESC 'Group membership'
   ```

```
SYNTAX 1.3.6.1.4.1.1466.115.121.1.12)

# Standard object classes from RFC2256

# RFC 2377
objectclass ( 1.3.6.1.1.3.1 NAME 'uidObject'
        DESC 'RFC2377: uid object'
        SUP top AUXILIARY MUST ( uid $ memberof) )
```

2. On the server, configure the group(s) assigned to each user with one entry for each group, either in a user definition file in the /etc/openldap directory, as shown in the following example, or on the command line.

```
dn: cn=<username>,dc=qa,dc=<domain>,dc=com
uid: <username>
cn: <username>
...
memberof: cn=<Group1>,dc=<domain>,dc=<domain>,dc=com
memberof: cn=d<Group2>,dc=<domain>,dc=<domain>,dc=com
memberof: cn=<Group3>,dc=<domain>,dc=<domain>,dc=com
...
homeDirectory: /home/<username>
```

NOTE: To give a user administrative access to the SP manager, assign the admin group name in a memberof definition.

Configuring group authorization for RADIUS authentication

The two tasks listed below must be done to configure groups for RADIUS authentication.

- The RADIUS server's administrator must define the desired groups and assign users to the groups.

  See *To configure groups on a RADIUS authentication server:* on page 137.

- The SP manager's administrator must configure the RADIUS server on the SP manager.

  The following list defines the values to define when configuring a RADIUS authentication server on the SP manager as shown below.

  auth1 *server*[:*port*] *secret* [*time-out*] [*retries*]

  acct1 *server*[:*port*] *secret* [*time-out*] [*retries*]

where:

auth1: The first RADIUS authentication server.

acct1: The first RADIUS accounting server.

server: The RADIUS server address.

port: Optional. The default port name is radius and is looked up through /etc/services.

secret: The shared password required for communication between the SP manager and the RADIUS server.

retries: The number of times each RADIUS server is tried before another is contacted.

time-out: The default is 3 seconds. How long the SP manager should wait for the RADIUS server's response.

To configure groups on a RADIUS authentication server:

1. On the server, open the /etc/raddb/users file for editing.
2. Assign groups to a user in the Framed-Filter-Id attribute.
3. Use the format Framed-Filter-Id=:group_name=<Group1>[,<Group2>,..., <GroupN>];, as shown in the following example.

```
groupuser1
Auth-Type= Local, Password =”xxxx”
Service-Type=Callback-Framed-User,
Callback-Number=”305”,
Framed-Protocol=PPP,
Framed-Filter-Id=”:group_name=<Group1>[,<Group2>,..., <GroupN>];”,
Fall-Through=No
```

NOTE: If the Frame-Filter-Id already exists, append the group_name declaration to the string starting with a colon (:). Make sure a final semicolon (;) is at the end of the declaration, as shown in the example.

4. Save and quit the file.

To configure a RADIUS authentication server on the SP manager:

1. Log into the console as root.
2. Open the /etc/raddb/server file for editing or create the file.
3. Make an entry for the RADIUS server (auth1), an accounting server (acct1) and if desired, make an entry for a second RADIUS authentication server (auth2) and for a second accounting server (acct2), by performing the following steps for each server.
4. Follow the file configuration directions shown in the following example.

```
# For proper security, this file SHOULD have permissions 0600,
# that is readable by root, and NO ONE else. If anyone other than
# root can read this file, then they can spoof responses from the
server!
# #
There are 3 fields per line in this file. There may be multiple
# lines. Blank lines or lines beginning with '#' are treated as
# comments, and are ignored. The fields are:
#
# server[:port] secret [timeout]
#
# the port name or number is optional. The default port name is
# "radius", and is looked up from /etc/services The timeout field is
# optional. The default timeout is 3 seconds.
#
# If multiple RADIUS server lines exist, they are tried in order. The
# first server to return success or failure causes the module to return
# success or failure. Only if a server fails to response is it skipped,
# and the next server in turn is used.
#
# The timeout field controls how many seconds the module waits before
# deciding that the server has failed to respond.
#
# server[:port] shared_secret timeout (s)
# 127.0.0.1 secret 1
# other-server other-secret 3
OUR.RADIUS.SERVER.IP:1645 OurSecret 1 3
```

5. Enter the IP address for the server.
6. (Optional) Define an alternate port.
7. Enter the secret (shared password).
8. (Optional) Enter a value to redefine the time-out.
9. (Optional) Enter a value to redefine the number of retries.

The following screen example shows entries that define the RADIUS authentication server and the accounting server to be the same server with the same IP address, sets the secret to cyclades, the time-out to 5 seconds and the number of retries to 5.

```
auth1 172.20.0.2 cyclades 5 5
acct1 172.20.0.2 cyclades 5 5
```

NOTE: Always configure both parameters auth1 and acct1.

10. Save and quit the file.

NOTE: Multiple RADIUS servers can be configured in this file. The servers are tried in the order in which they appear. If a server fails to respond, the next configured server is tried.

Configuring group authorization for TACACS+ authentication

The two tasks listed below must be done to configure groups for TACACS+ authentication.

- The TACACS+ server's administrator must define the desired groups and assign users to the groups.
- The SP manager administrator must configure the TACACS+ server on the SP manager. The administrator of the SP manager, must configure the TACACS+ authentication server for raw access. Table 6.5 lists two ways to perform the needed configuration.

Table 6.5: Methods for Configuring the TACACS+ Authentication Server for Raw Access

Method	Where Documented
Web Manager	*To Configure a TACACS+ Authentication Server [Expert]* on page 286 **NOTE:** Make sure to check the *Enable Raccess Authorization* checkbox.
SP manager **command line**	*Configuring a TACACS+ authentication server on the SP manager* on page 140

The following cli utility command line can also be used to configure a server for raw access:

```
cli> set auth tacplus service raccess
```

To assign a group to a user on the TACACS+ server:

1. Add a definition for the group to the authentication authorization accounting (AAA) database on the TACACS+ server.

NOTE: These additions can be made through a GUI. The example shows the configuration if a GUI is not available.

```
##############################################################
#  Group Definitions
##############################################################
group = group_name {
...
}
```

2. To the definition for each user, add the raccess service in the form service = raccess and assign the desired group to the user in the form member = group_name.

NOTE: Each user may belong to only one group. To give a user administrative access to the SP manager, assign the admin group.

```
##############################################################
#  User Definitions
##############################################################
user = username {
   service = raccess
   member = group_name
}
```

Configuring a TACACS+ authentication server on the SP manager

The following list defines the values that must be defined in the SP manager's /etc/tacplus.conf file.

- authhost1: IP address of the TACACS+ authentication server. A second TACACS+ authentication server can be configured with the parameter authhost2.
- accthost1: IP address of a TACACS+ accounting server, which can be used to track how long users are connected after being authorized by the authentication server. Its use is optional. If this parameter is not defined, accounting is not be performed. If the same server is used for authentication and accounting, both parameters must be defined with the same address. A second TACACS+ accounting server can be configured with the parameter accthost2.
- secret: The shared secret (password) necessary for communication between the SP manager and the TACACS+ servers.
- encrypt: The default is 1, enable encryption. A value of 0 means disable encryption.
- service: The service to be enabled, in this case: raccess.
- protocol: The default is lcp (line control protocol). Specify another parameter if required.

- timeout: The time-out (in seconds) for a TACACS+ authentication query to be answered.
- retries: Defines the number of times a TACACS+ server is tried before another is contacted. The first server authhost1 is tried for the specified number of times, before the second authhost2, if configured, is contacted and tried for the specified number of times. If the second server fails to respond or if no second server is configured, TACACS+ authentication fails.

To configure a TACACS+ authentication server on the SP manager:

1. Log into the console as root.
2. Open the /etc/tacplus.conf file for editing.
3. Change the values described under *Configuring a TACACS+ authentication server on the SP manager* on page 140.

NOTE: To configure group access on the TACACS+ authentication server, service must be defined as raccess.

4. Save and quit the file.

CHAPTER 7

Using the cli Utility

cli Utility Overview

An administrator can configure the SP manager using the cli utility. Only one administrator can be logged into the SP manager at a time. While in the cli utility, an administrator can escape to the shell and when finished can return to the cli utility.

Administrators often prefer using the cli utility over the Web Manager because they can run frequently performed cli configuration commands from shell scripts or from text files that can be executed in batch mode. For example, on an SP manager with 40 private Ethernet ports, configuring all the SPs one by one could be tedious and prone to error, so scripting the configuration of multiple SPs is a good use of the cli utility. Example scripts are provided in /libexec/example_scripts.

The cli utility provides a set of commands (described under *cli Commands* on page 149) that act on parameters nested in a format called the CLI parameter tree. Some parameters require arguments when the parameters are entered with some commands.

NOTE: This section describes the cli commands and how to navigate the cli parameter tree, but it does not describe all the parameters and values. For examples of how to use the cli command for performing tasks such as adding users and groups, configuring devices and authentication, see examples in /libexec/example_scripts.

Execution Modes

The cli utility has three modes: a command line mode, interactive mode and batch mode.

Command line mode

Command line mode refers to when the cli utility is invoked on the Linux command line with options, commands, parameters and values.

The cli utility performs the specified commands, displays any values requested by a command (such as the get command) and returns the shell prompt. To commit the changes made in command line mode, make sure to use the -C option as part of the command line.

When invoked without commands, cli enters interactive mode; see Interactive mode. When the cli utility is invoked with the -f <file> option or is invoked from a script, the commands are executed in batch mode from the specified file or script.

Interactive mode

Entered by invoking cli on the command line. The cli> prompt appears, and the administrator performs configuration by entering commands followed by parameters followed by parameter arguments at the cli> prompt. The cli utility waits for new commands until the user enters the quit or exit command.

Batch mode

Refers to invoking cli commands from a file as follows:

- cli commands can be saved in a plain text file and executed in batch mode by invoking the cli utility with the -f <file> option.
- cli commands can be used in any kind of shell script:
  - #!/usr/bin/cli can be invoked at the top of a shell script if the script contains only cli commands.
  - Any type of shell can be used to run cli commands along with other commands.

cli Options

Administrators can invoke the cli command with a number of different options shown in the following table.

Table 7.1: cli Utility Options

Option	Description
-1	When entered either in command line or in batch mode with commands that act on a single parameter, speeds up response time.
-C	Commits changes when quitting.
-f <file>	Reads commands from file. Used for running commands in batch mode.
-F	Forces login (terminate an existing configuration session, if any). Used when specifying commands to run in command line or batch mode.
-h	Help. Shows a brief summary of command line options.
-q	Quiet mode. Suppresses messages. Useful only when entering interactive mode.
-t <time-out>	Sets the idle time-out in minutes. Default is 10 minutes.
-T	Disables idle time-out (same as -t 0).
-V	Displays the cli version and exits.

Table 7.1: cli Utility Options

Option	Description
--	Signals the end of options and start of cli commands. If any are specified, cli goes into command line or batch mode.

cli Parameters and Arguments

The CLI configuration options are organized in a hierarchy called a parameter tree. You can use the get, show and list commands to show parameters. You can also use the get command to show the values of individual parameters at the end of a branch.

The following diagram illustrates one parameter in the SP manager cli parameter tree. As shown in the example in Figure 7.1, each branch in the parameter tree is made up of one or more parameters, one nested below the other. In the figure, the top-level network parameter is followed by the second-level interface parameter, which is then followed by the third-level failover parameter. No parameters are nested under failover.

network
interface
failover

Figure 7.1: Example Branch in the cli Parameter Tree

In this branch, the only commands supported are get and set. All of the parameters in a branch are entered together on a single cli command line. For example, to get the value set for failover, you would enter the following command:

```
cli> get network interface failover
no
cli>
```

Entering set with yes enables Ethernet failover; no disables it. To set failover, you would enter the following command in interactive mode:

```
cli> set network interface failover yes
OK
cli>
```

You can use autocompletion with the set command to find out the accepted values.

```
cli> set network interface failover <Tab><Tab>
set to yes or no. Enables or disables the interface bond0.
cli>
```

Entering values with parameters

Enter values that contain spaces within double quotes (**"**). To set a value containing double quotes, precede the double quote within a double quote with a backslash (****), which is achieved by typing two backslashes.

To add a user called mozart and to set the value of the user's GECOS to "Wolfgang Amadeus "Wolfie" Mozart, \\ Vienna, Austria //," you would enter the following:

```
cli> add spmanager user mozart
OK
cli> set user mozart gecos "Wolfgang Amadeus \"Wolfie\" Mozart,
\\\\\"Vienna, Austria\"\/\/\"
OK
```

Entering a command in interactive mode

Based on the branch in the example in Figure 7.1, you could enter the set command with the following parameters in interactive mode to turn on Ethernet failover.

```
[admin@MergePoint5224 /home/admin]# cli
cli> set network interface failover yes
```

Entering a command in command code

Based on the branch in Figure 7.1, you could enter the set command to turn on Ethernet failover with the parameters shown in the following screen example in command mode. When the command completes, the shell prompt returns. The backslash in the example indicates that the command is too long for the page format. On the command line, you could enter all the parameters together with the value on the same command line.

```
[admin@MergePoint5224 /home/admin]# cli -CF1 set network \
interface failover yes
```

Entering a command in batch mode

Based on the example in Figure 7.1, you could use batch mode to turn on Ethernet failover as shown in the following examples.

Example cli shell script

Start the script by entering #!/usr/bin/cli with the **-**CF options.

```
#!/usr/bin/cli -CF
set network interface failover yes
```

You could then make the script executable and execute it on the command line, as shown in the following example.

```
[root@MergePoint5224 /]# chmod 777 scriptname1
[root@MergePoint5224 /]# ./scriptname1
```

Example bash shell script

If you want to run a cli command from the same script that is running other Linux commands, you could put the command in another type of shell script. The bash shell is shown in the following example.

```
#!/bin/bash
...
/usr/bin/cli -CF -- set network interface failover yes
...
```

If you want to run multiple cli commands from a script that is also running other Linux commands, you could add the multiple cli commands as shown in the following example.

```
#!/bin/bash
...
/usr/bin/cli << EOF
set network interface failover yes
set network hostname frutabaga
commit
EOF
```

You could then make the script executable and execute it on the command line, as shown in the following screen example.

```
[root@MergePoint5224 /]# chmod 777 scriptname2
[root@MergePoint5224 /]# ./scriptname2
```

Example plain text file

You can put one or more commands in a plain text file without invoking any shell as shown in the following screen example.

```
set network interface failover yes
```

And then you can invoke the cli command with the **-**f <file> option to execute the command(s) from the file, as shown in the following example.

```
[root@MergePoint5224 /]# cli -f filename
```

Autocompletion

Autocompletion can be used to find out what commands and parameters are available. Pressing the **Tab** key displays all the commands at the top level, as shown in the following screen example.

```
cli> <Tab>
add    commit   exit  list   rename    set   show
cd     delete   get   quit   revert    shell version
```

Typing any of the commands such as add or set then pressing **Tab** twice displays all the top level parameters, as shown in the following screen example.

```
cli> set <Tab> <Tab>
adsap2     event_notify   logpipe         pptd          sshd
auth       group          network         profile       syslog
auxport    httpd          notifications   sensoralarm   timezone
bootconf   ipdu           ntp             service       user
cards      ipsec          onboard         snmpd         web
dhcpd      iptables       param           spmanager
```

Pressing the **Tab** key once after partially typing a parameter name automatically completes the parameter name, unless there is more than one parameter name beginning with the typed characters. If more than one parameter name begins with the typed characters, then **Tab Tab** displays them all.

NOTE: adsap2, dhcpd, and logpipe are not customer**-**configurable. onboard is listed for backwards compatibility to scripts written for earlier versions of this product when it was the Cyclades OnBoard Service Processor Manager.

Examples

```
cli> s<Tab><Tab>
set   shell   show
cli> se<Tab>
cli> set n<Tab><Tab>
network notifications ntp
cli> set ne<Tab>
cli> set network <Tab><Tab>
hostname hosts interface resolv smtp st_routes
cli> set network i<Tab>
cli> set network interface eth0 <Tab>
active address broadcast gateway method mtu netmask
cli> set network interface eth0 ac<Tab>
cli> set network interface eth0 active <Tab>
enable or disable eth0 with yes or no
cli> set network interface eth0 active <Esc> <Tab>
cli> set network interface eth0 active yes <Tab>
active address broadcast gateway method mtu netmask
cli> set network interface eth0 active yes b<Tab>
cli> set network interface eth0 active yes broadcast 10.0.0.255<Enter>
OK
```

cli Commands

The cli utility supports the commands that are described in the following sections with examples.

```
cli> <Tab><Tab>
add       commit   exit   list   quit     revert   shell   version
cd        delete   get    move   rename   set      show
```

add

The add command adds the last parameter and sets it to the default value (if any). Any non-default values must be set using the set command.

The add command is used instead of set when multiple parameters of the same type can exist. For example, add network hosts IP address makes an entry for a host with the specified IP address in the hosts list. In that case, add is used because multiple hosts can exist.

In contrast, the set command (as in: set network interface eth0 <IPaddress>) is used to specify the IP address for the eth0 Ethernet interface. In that case, the set command is used because each interface has only one IP address.

Adding certain parameters causes one or more related parameters to be added to the subtree. For example, when an IP address is added to the hosts list, empty hostname and alias parameters are also added. For some parameters, a set of meaningful default values are assigned. For empty parameters, the get or show commands list the parameter names without any values.

You must add parameters in a prescribed order. For example, because an empty hostname and alias parameters are created when you add a host's IP address, you cannot add a host by name before specifying the host's IP address, and you cannot specify the host name at the same time as its IP address. To specify a name or alias for a host you need to add the host first by adding its IP address, then you need to use the set command to specify its name and alias.

Synopsis

```
add parameter(s) value(s)
```

Examples

```
cli> set network hosts 192.168.160.11 name fruitbat
ERR result=5 No such file or directory
cli> get network hosts 192.168.160.11 name fruitbat
ERR result=5 No such file or directory
cli> add network hosts 192.168.160.11
OK
cli> get network hosts 192.168.160.11
name
alias
cli> set network hosts 192.168.160.11 name fruitbat alias fbat
OK
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name: fruitbat
network hosts 192.168.160.11 alias: fbat
```

Parameters that can be added

The following table shows the parameters that can be added using the add command. Table 7.3 on page 158 shows additional parameters and values that must be set for each parameter after the parameter is added. When a parameter is shown in the Parameter Level 2 column, the Parameter Level 1 and Parameter Level 2 parameters must be entered together with the add command, for example to add an ipsec connection you need to enter both ipsec and conn followed by the connection name: add ipsec conn <connection_name>; the connection must then be configured after adding, using the set command.

Table 7.2: Parameters That Work With the cli add Command

Parameter Level 1	Parameter Level 2	What It Configures [Syntax]
adsap2	authserver	An ADSAP2 authentication server(s). **NOTE:** Not configurable on the SP manager, used by DSView 3 management software.
	state	The ADSAP2 state (secure or trust - all). **NOTE:** Not configurable on the SP manager, used by DSView 3 management software.
group		Adds a group to the list of local groups.The group name is automatically assigned a group ID. [add group <groupname>]
ipsec	conn	Adds a VPN IPSec connection. [add ipsec conn <connection_name>]
iptables	nat | filter	Adds chainname to the list of chains. [add iptables <nat | filter> <chainname>] Also can be used to add a rule number. [add iptables <nat | filter> <chainname> <number>] **NOTE:** By default, a set of chains is defined with hidden rules: For NAT, the predefined chains are: PREROUTING, POSTROUTING, OUTPUT. For filter, the predefined chains are: INPUT, OUTPUT, FORWARD.
network	hosts	Adds an IP address for a host. [add network hosts <IPaddress>]
	st_routes	Adds to the list of static route targets a subnet or host (networks in the form 1.2.3.4/255.255.0.0 or host IPs). [add network st_routes <network_IPaddress/netmask> | <host_IPaddress>]
notifications		Adds a notification using any name. [add notifications notification_name]
onboard [See spmanager]		**NOTE:** The onboard parameter is maintained only for backward compatibility.

Table 7.2: Parameters That Work With the cli add Command (Continued)

Parameter Level 1	Parameter Level 2	What It Configures [Syntax]
snmpd	rwcommunity | rocommunity	Adds a read-write community [rwcommunity] or a read-only community [rwcommunity]. {add snmpd <rwcommunity | rocommunity> <community_name>]
	rwuser | rouser	Adds a read-write user [rwuser] or a read-only user [rouser]. [add snmpd <rwuser | rouser> <user_name>]
	user	Adds a user and fills in the subtree with default values and randomly generated passwords.[add snmpd user <user_name>]
	group	Adds a group. [add snmpd group <group_name>]
	view	Add a view: add snmpd view <view_name>. [add snmpd view <view_name>]
	access	Add an access type. [add snmpd access <noauth | auth | authpriv>]
	proxy	Add a snmpd proxy. [add snmpd proxy <proxy_name>]
spmanager	server	Add a managed device. [add spmanager server <device_name>]
	user | group	Add the name of a user or group authorized to access the device. [add spmanager user <username> OR add spmanager group <groupname>] Add a device to configure access for an existing user or group (after the device has been configured as described under spmanager server). [add spmanager user | group <device_name>]
syslog	destination	Adds the name of syslog server to the default console or rootuser destinations defined for syslog messages. [add syslog destination <server_name>]
user	**NOTE:** Do not use. The correct way to add a user using the cli is as a spmanager user, as in: **add spmanager user joe**	Add a user or users to the list of local users; add user <username>.

cd

Set a parameter prefix for subsequent commands. The prompt then changes to indicate the prefix. Entered by itself, cd returns to the top level.

Synopsis

```
cd [parameter(s)]
```

Examples

```
cli> cd network
network> get hostname
dingo
network> set hostname kookaburra
OK
network> cd interface eth0
network interface eth0> set
active    address   alias     broadcast  gateway   method    mtu
netmask
ip address for interface eth0
netmask for interface eth0
network interface eth0> set address 192.168.160.10 netmask \ 255.255.255.0
OK
network interface eth0> cd ..
network interface> cd eth1
network interface eth1> set address 192.168.50.10
OK
network interface eth1> cd
cli>
```

commit

Saves changes in configuration files and creates a compressed copy of the configuration files in a backup directory.

NOTE: If you make a change but do not commit it, the configuration files are not updated, and your changes will be lost after the next reboot.

Synopsis

```
commit
```

delete

Deletes the last parameter in the command line. Deleting certain parameters deletes associated parameters. For instance, if an IP address is deleted from the host list, other parameters associated with a host (name, alias) are also deleted.

Synopsis

```
delete parameter(s)
```

Some parameters cannot be deleted. Parameters that can be added can be deleted.

Examples

```
cli> get network hosts 192.168.160.11
network hosts 192.168.160.11 name fruitbat alias fbat
cli> delete network hosts 192.168.160.11
OK
cli> set network hosts 192.168.160.11 name: fruitbat
ERR result=5 No such file or directory
cli> get network hosts 192.168.160.11 alias: fbat
ERR result=5 No such file or directory
```

get | show

Get the value assigned to a parameter. When no parameters are listed, the whole parameter tree is displayed. If full parameters are specified, the assigned value is displayed.

Synopsis

```
get | show parameter(s)
```

Examples

```
cli> get network hostname
anchovy
cli> show network resolv domain
avocent.com
```

When get is entered with a partial parameter, all the subtrees display. In the output, if a value is assigned, the parameter preceding the value ends with a semicolon.

```
cli> get network
network interface failover: no
network interface eth0 active: yes
network interface eth0 method: dhcp
...
network smtp auth method
network ipv4 icmp echo_ignore_all: 0
network ipv4 ip forward
cli>
```

If the system assigns default values, default values are shown next to the automatically added parameter name, as in the following example, which was entered on the SP manager before any configuration has been done.

```
cli> get network interface eth0
network interface eth0 active: yes
network interface eth0 method: dhcp
network interface eth0 address: 192.168.160.10
...
network interface eth0 gateway: none
network interface eth0 mtu: 1500
cli>
```

NOTE: If you make a change but do not commit it (see *commit* on page 153), the configuration files are not updated. The get command shows the changes that are currently stored in the RAM memory, not the actual value stored in the affected configuration file.

list

List available parameters. With no parameters listed, the whole parameter tree is displayed. If parameters are specified, the corresponding subtree is displayed.

Synopsis

```
list parameter(s)
```

Example

```
cli> list network hostS
network hosts 127.0.0.1 name
network hosts 127.0.0.1 alias
network hosts 192.168.160.10 name
network hosts 192.168.160.10 alias
```

quit | exit

Quit cli. (**Ctrl+d** also quits the cli utility.) If changes have not been committed, the user is prompted to commit the changes or quit without committing.

Synopsis

quit

Example

```
cli> set network hostname frutabaga
OK
cli> quit
You have made changes but haven't committed them yet.
```

```
To commit the changes, use the “commit” command.
To revert all changes and quit without committing, use “quit!”.
cli> commit
cli> quit
```

quit!

Quit the cli utility, discarding any uncommitted changes.

rename

Rename a parameter. Depending on the parameter, this may result in a whole subtree of parameters being moved. For instance, if an IP address in the host list is changed, all parameters associated with that host (name, alias) are moved under the new name.

Synopsis

```
rename parameter(s) value(s)
```

Examples

```
cli> get network hosts 192.168.160.11
network hosts name: fruitbat
alias
cli> rename network hosts 192.168.160.11 192.168.160.222
OK
cli> get network hosts 192.168.160.11
ERR No such file or directory
cli> get network hosts 192.168.160.222
name fruitbat
alias
```

revert

Discard changes and revert to previously committed state.

Synopsis

```
revert
```

Examples

```
cli> get network hostname
dingo
cli> set network hostname kookaburra
OK
cli> get network hostname
kookaburra
cli> revert
OK
```

```
cli> get network hostname
dingo
```

set

Set the value(s) of the last parameter. When multiple parameters are specified in one command, either all are set successfully or none of the values are changed.

The set command is used to set an existing value, in contrast to add command which is used to add something to the parameter tree. For example, this set command is used to specify the IP address for an Ethernet interface which already is identified by the eth0 parameter in the parameter tree: set network interface eth0 <IPaddress>. In contrast, new hosts need to be added with the add command before their parameters can be specified; add network hosts <IPaddress> makes an entry for a host with the specified IP address in the hosts list. Parameters for this new host can then be changed with the set command: set network hosts <IPaddress> name <hostname>.

Synopsis

```
set parameter(s) value(s)
```

Examples

```
cli> set network resolv dns0 10.0.0.1
OK
cli> set network interface eth1 active yes address 10.0.0.3 netmask \
255.255.255.0 broadcast 10.0.0.255
OK
cli> set
network interface eth0 active yes eth1 active yes
ERR sanity check failed
```

shell

Escape to shell. This command is only available to root.

Synopsis

shell

Examples

```
cli> shell
[root@MergePoint5224 root]# whoami
root
[root@MergePoint5224 root]# logout
cli>
```

version

Displays the current cli version.

Synopsis

version

Examples

```
cli> version
MergePoint5224 CLI 2.0 (2005-06-16T13:47+1000)
```

Summary of How to Configure the Top Level Parameters

This section provides a brief overview of how to configure the top level parameters.

Table 7.3 describes which of the top-level parameters that you can set without using the add command first, and it also shows the parameters that need to be set after the add command creates the parameter to set additional parameters and values.

Table 7.3: Setting Top Level cli Parameters

Parameter	Command
adsap2	**NOTE:** Not configurable on the SP manager, used by DSView 3 management software.
auth	• Use the set command with the auth type parameters to set an authentication type for logins to the SP manager, either krb5, ldap, nis, radius, smb, tacplus (set auth type <krb5 | ldap | nis | radius | smb | tacplus>). • Use the set command with the auth type ppp parameters to set an authentication type for logins through AUX port-connected or PC card modems. **NOTE:** Authentication types supported for the SP manager and for target devices are listed in Table 4.1, “Supported Authentication Types,” on page 22. • Use the set command with the auth parameter to configure authentication servers to be used either by the SP manager or target devices (set auth <authtype> type **Tab Tab** shows what parameters need to set for each type of authentication server).
auxport	Use the set command to configure the AUX port profile for a connected modem or IPDU (set auxport profile <none | modem | ipdu>). If the modem profile is set, use the set command to configure the modem (set auxport modem **Tab Tab** shows the modem configuration parameters to set).
bootconf	Use the set command to configure boot configuration (set bootconf **Tab Tab** shows the boot configuration parameters to set). To set the speed for the public Ethernet ports use set bootconf fecmode<N> option (set bootconf fecmode[1 | 2] [auto, 100H | 100F | 10F | 10H]).

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
cards	Use the set command to configure PC cards (set cards **Tab Tab** shows the cardtypes; set cards <cardtype> **Tab Tab** shows the configuration parameters to set).
dhcpd	Not supported.
group	After the add command is used to add a group, or when configuring a default group, use the set group <groupname> members command to configure the group members (set group <groupname> members <username>[, <username>, ..., <username>) (set group **Tab Tab** shows the existing groups; set group <groupname> shows the parameters to set for groups).
httpd	Use the set command to enable or disable and configure HTTP/HTTPS services (set httpd http **Tab Tab** shows the configuration parameters to set).
ipdu	• Use the set command to configure an IPDU or to configure the outlets (set ipdu s1 **Tab Tab** shows the configuration parameters to set) • Use the add command to add users who can configure outlets (add ipdu s1 users <username>). • Use the set command to configure which outlets each user can manage (set ipdu s1 users <username> **Tab Tab** shows the configuration parameters to set).
ipsec conn	After the add command is used to add an IPSEC connection name, use the set command to configure the connection parameters (set ipsec conn <connectionname> **Tab Tab** shows the configuration parameters to set). **NOTE:** The key parameter can be specified in hexadecimal (with the 0x prefix followed by any of: a-f, A-F, 0-9), in base 64 (with the 0s prefix followed by any base 64 number using a-z, A-Z, +, or \); or in a text string (entered with the 0t prefix followed by text).

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
iptables [filter | nat]	**NOTE:** By default, a set of chains is defined with hidden rules: For NAT, the predefined chains are: PREROUTING, POSTROUTING, OUTPUT. For filter, the predefined chains are: INPUT, OUTPUT, FORWARD. For background information, see *Firewall/Packet Filtering on the MergePoint 5224/5240 SP Manager* on page 53 and Table 4.19 on page 54. Use the set command to configure a rule for a predefined chain after the add command is used to a rule for that chain. Or use the set command to configure a rule after the add command is used to add a new chain and to add a new rule for the new chain (set iptables <filter | nat> **Tab Tab** shows the current chains; set iptables <filter | nat> <chainname> shows the rules for a specific chain, and get iptables <filter | nat> <chainname> <rule_number> shows the configuration parameters to set filtering policies. **NOTE:** For NAT and filter, the following target actions are defined: DROP, ACCEPT, REJECT or chainname. For NAT, the following additional target actions are defined: DNAT to change the destination address [DNAT to-destination <IPaddress>]; and SNAT, to change the source IP [SNAT to-source <IPaddress>].
network hostname	Use the set command to configure the hostname for the SP manager (set network hostname <hostname>). **NOTE:** By default the hostname is MergePoint<model_number> as in MergePoint 5224.
network hosts	After the add command is used to add a host to the hosts table (add network hosts <IPaddress>), use the set command to configure the host's IP address and optional alias (set network hosts <IPaddress> **Tab Tab** shows the parameters to set).
network interface	Use the set command to configure one of the network interfaces (set network interface **Tab Tab** lists the interfaces to configure (set network interface <interface_name> **Tab Tab** lists the parameters to configure).
network ipv4	Use the set command to configure ipv4 (set network ipv4 **Tab Tab** lists the parameters to configure).
network resolv	Use the set command to configure DNS domain and one or more DNS servers (set network resolv **Tab Tab** lists the parameters to configure).

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
network smtp	Use the set command to configure email notifications to be sent to root (set network smtp **Tab Tab** lists the parameters to configure).
network st_routes	After using the add command to add a static route to the routing table, use the set command to configure the static route (set network st_routes <IP_address> **Tab Tab** shows the parameters to set).
notifications	After using the add command to add a notification, use the set command to specify a trigger using the format used for triggers in the /etc/syslog.ng file [set notifications <notification_name> trigger <trigger_string>]; a notification type, one of SNMP, SMS or MAIL [type <SNMP|SMS|MAIL>].
	If MAIL is the notification type, use the set command to set the recipient email address. [set notifications <name to <email_address>]; sender email address [from <email_address>]; Subject: line in quotes [subject "<subject of the notification email>"]; email message body in quotes [body "<body of the email message>"]; mail server <IP_address> [<mail_server_IP_address>].
	If SNMP is the notification type, use set notifications snmptrap with an OID [oid <OID>]; trap number [trapnumber <number>]; community name [community <community_name>]; server IP address [<server_IP_address>]; message body in quotes [body body of the email message].
	If SMS is the notification type, use set notifications pager with a pager number [number pager_number], message body in quotes [body body of the pager message]; username [user username]; server IP address [server IPaddress]; port number [port number].
sensoralarm	After using the add sensoralarm command to configure a sensor alarm (add sensoralarm <alarm_ID>). use set sensoralarm to configure the parameters (set sensoralarm <alarm_ID> **Tab Tab** shows the parameters to set). Enter the name of a sensor on the device in quotes (such as Sys Fan 1) and set an appropriate range if you specify inside or outside parameters.
service	Use the set service command to enable or disable any service (inetd, ssh, ntp, snmpd, ipsec, syslog, pmd, pptpd, rpc, apache, dhcpd, adsap2, evtgen, logpipe). [set service <service_name> <enable | disable>].

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
snmpd [access | com2sec | group | user | view]	After using the add snmpd command to add access, com2sec, group, user and view, use the set snmpd command to configure the parameters (set snmpd <parameter> **Tab Tab** shows the parameters to set).
spmanager global default authtype	Use the set command to configure the authentication method for SP manager logins (set spmanager global default authtype <authentication_method>).
spmanager global default databuf	Use the set command to configure the default for data buffering (set spmanager global default databuf [yes | no]).
spmanager global security encrypt_passwords	Use the set command to configure whether passwords are encrypted; the default is no (set spmanager global security encrypt_passwords [yes | no]).
spmanager global security override_authorization	Use the set command to configure whether authorizations are ignored when users attempt to access devices; the default is no (set spmanager global security override_authorizations [yes | no]).
spmanager global sort server	Use the set command to configure the sort method for the names of devices, either alphabetical or no sorting. By default, device names appear in the order they were configured (set spmanager global sort server <alpha | none>).
spmanager global strict subnet	Use the set command to configure whether or not sanity checks are made for the subnet IP and netmasks. If set to no, overlapping subnets are allowed. (set spmanager global strict subnet <yes | no>).
spmanager global strict uniqip	Use the set command to configure whether or not sanity checks are made to ensure that the real IP assigned to a device is unique. (set spmanager global strict uniqip <yes | no>).
spmanager group	After using the add command to configure an spmanager group, use the set command to configure the parameters (set spmanager group <groupname> **Tab Tab** shows the parameters to set).
spmanager server	After using the add command to configure a device, use the set command to configure the parameters. (set spmanager server <devicename> **Tab Tab** shows the parameters to set). For example, the set spmanager server <devicename> databuf <yes | no | default>] command configures whether data buffering is done according to the global setting or not.

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
sshd protocol	Use the set sshd protocol command to set the SSHD protocol version to either 1 or 2 or both (1,2 or 2,1). Default is 2,1. [set sshd protocol <version[,version]>]
spmanager user	After using the add spmanager user command to configure a user, use the set user command to configure the normal Linux user's parameters such as passwd (set user <username> **Tab Tab** shows the parameters to set). Also use the add spmanager user command to authorize an existing user to use a previously configured device (add spmanager user <username> <devicename>), then use the set spmanager user <username> <devicename> command to specify which device management actions the user can perform on the device (console, directcommand, nativeip, nci, power, sel, or sensors, specifying yes or no for each). [set spmanager user <username> <devicename> console <yes | no> directcommand <yes | no> nativeip <yes | no> nci <yes | no> power <yes | no> sel <yes | no> sensors <yes | no>]
syslog destination	Use the set syslog destination command parameters to configure a syslog destination (either the SP manager console or rootuser or a syslog server name that has been added using the add syslog destination <syslog_server_name> command). Also use the set destination <destination_name> command to enable or disable the destination [enable <yes | no>]; set a destination type, one of tcp, udp, or file [type <tcp | udp | file>]; set a valid username as the owner of the tty [usertty <username>]; set an IP address for the syslog server [tcp|udp <IP_address>]; set a destination filename for the syslog [file <filename>]; set a named pipe or a template as a destination [pipe <pipename>].
syslog filter	Use the set syslog filter command to enable a syslog filter level. [set syslog filter <sysfilter | webfilter> level <emerg | alert | crit | err | warn | notice | info|debug | <level_number> <yes | no>]
timezone	Use the set timezone command to specify the timezone using a file relative to /usr/share/zoneinrfro, for example Etc/UTC. (set timezone <file>]
user	• Do not use this command to add a user. Use add spmanager user <username> first. • Use the set user command to configure the normal Linux user's parameters such as the passwd (set user <username> **Tab Tab** shows the parameters to set).

Table 7.3: Setting Top Level cli Parameters (Continued)

Parameter	Command
web help-prefix	Use the set web help-prefix command to specify a user-accessible web server location where the help files have been downloaded), so the Web Manager can locate the help files when a user clicks the help button. The default help-prefix is http://www.cyclades.com/online-help. [set web help-prefix <URL>]
web browser_timeout	Use the set web browser_timeout command to specify a number of seconds of inactivity before a Web Manager login session is ended. If the specified period of inactivity occurs while a user is logged into the Web Manager, the user is automatically logged out of the Web Manager. Any DirectCommand sessions are automatically terminated. [set web browser_timeout <seconds>]. See *Changing Web Manager Time-outs* on page 131 for details and examples.
web session_timeout	Use the set web session_timeout command to specify a number of seconds of inactivity before a Web Manager login session is ended without forcing a logout unless the user clicks any of the Web Manager controls. Preventing user activity without automatic logouts allows DirectCommand sessions to continue. Default: no setting. [set web session_timeout <seconds>] See *Changing Web Manager Time-outs* on page 131 for details and examples.

APPENDICES

Appendix A: Troubleshooting

Port Mapping Fails When Using DirectCommand

This section describes some considerations that may apply if port mapping fails when a user attempts DirectCommand access to a target device.

If DirectCommand is invoked by an unprivileged user (such as a regular user on a UNIX-based system), DirectCommand may not be able to open privileged TCP ports (numbered below 1024). DirectCommand attempts to open the port by adding an offset to any requested port number that is less than 1024 and by automatically modifying the URL to represent the new local port. However, if the service provided by a target device can operate only on the original predetermined TCP port, DirectConnect does not work properly and displays a descriptive warning. If this occurs, DirectConnect connections may be made to the target device only by workstation administrators.

Another possible cause for failed port mapping by Direct Command is that the user's workstation may be running an application that uses a TCP port that is needed by DirectCommand. For example, if the user's workstation is running a web server on port 80 and the target device being accessed through DirectCommand expects port 80 to be mapped, DirectCommand might not work. To prevent this kind of conflict, make sure that local applications running on the user's workstation do not use the same TCP port numbers used by DirectCommand.

Network failure

This section summarizes the options for connecting to the MergePoint 5224/5240 SP manager for troubleshooting in the event of an IP network failure.

Remote administrators can connect to the SP manager in case of network failure in any of the following ways:

- By bringing up the Web Manager or logging into the console over PPP after establishing a dial-in or callback connection to either of the following modem types:
  - An external modem optionally connected to the SP manager.
  - A modem on a PC modem card optionally installed in the SP manager
- By logging into the console after establishing a dial-in connection from a terminal emulation program to an external modem optionally connected to the SP manager.

Local administrators can connect to the SP manager by logging into the Linux command line through a terminal or workstation that is connected to the console port.

All of these connection methods must be previously configured as described elsewhere in this manual. For example, to make it possible to dial in if the network connection becomes unavailable, a modem must be installed and configured. Connecting to the console requires a terminal or a

computer with a terminal emulation program connected to the console port. All procedures in this appendix assume a login by the root user.

Login failure

If no one can log into the SP manager, you can perform the following procedure to reset the root or admin user's password. This procedure would be needed, for example, if an attempt to log into the console as root brings up the following message:

```
login[212]: FAILED LOGIN
1 FROM  FOR root, User not known to the underlying
authentication module
Login incorrect
```

To recover from login failure:

1. Make a terminal connection to the SP manager.
2. Turn power off and then on to physically reboot the SP manager.
3. When prompted, hit any key to interrupt the boot and enter U-Boot monitor mode.

   See *To boot in U-Boot monitor mode:* on page 203. The U-Boot monitor prompt appears as shown in the following screen example.

   ```
   [root@MergePoint5224 root]# reboot
   ...
   Hit any key to stop autoboot: 0
   =>
   ```

4. Boot in single-user mode.

   ```
   => hw_boot single
   ```

5. When single user mode comes up, use the passwd command to change the root or admin user's password.

   The following screen example shows changing the admin user's password.

   ```
   [root@(none)/]# passwd admin
   New password: admin_password
   Re-enter new password: admin_password
   Password changes
   passwd; password updated successfully
   [root@(none)/]#
   ```

6. Restart the SP manager to return to multiuser mode.

   ```
   [root@(none)/]# reboot
   ```

   The root or admin user should now be able to log in with the new password.

7. Reconfigure authentication as desired.

Web manager stops responding

If the Web Manager stops responding you can perform the following procedure to restart the Apache web server.

To restart the Web Manager:

1. Enter the **http -k start** command as shown in the following screen example.

```
[root@MergePoint5224 root]# /usr/local/apache2/bin/httpd -k start
```

2. Enter the **ps** command with the **-ef** option and look for a line with apache, as shown in the following screen example.

```
[root@MergePoint5224 /root]# ps -fe | grep apache
10131 nobody 3864 S /usr/local/apache2/bin/httpd -k start
```

   If a line like the bottom line in the previous screen example appears, the web application successfully restarted.

Firmware image is corrupted

Information in *Boot file location* on page 200 gives an administrator who knows the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

Network boots are recommended for troubleshooting only. For example, if you want to test a new release of the firmware to make sure a problem is fixed, or if the removable Flash memory becomes corrupted, you could download the firmware to a tftpboot server. After you test the image and replace the Flash, if needed, you can then save the firmware image to the removable Flash using the create_cf command.

You can use the create_cf command when troubleshooting problems with the boot image, as described under *To upgrade to a boot image from a network boot:* on page 204.

Appendix B: Technical Specifications

Table B.1: MergePoint 5224/5240 SP Manager Specifications

Hardware	
CPU	Freescale Power QUICC III
Memory	256 MB DDRAM/128 MB compact Flash
Interfaces	24/40 Ethernet 10/100 BT on RJ-45 1 RS-232 console on RJ-45 1 RS-232 DTE on RJ-45 for power manager or external modem 1 10/100/10000 BT Ethernet on RJ-45 (primary) 1 10/100 BT Ethernet on RJ-45 (optional secondary or failover)
Dual 32/16 bit PCMCIA Slots:	Supported PC card types listed at www.avocent.com
Enclosure	1U Steel
Dimensions (WxDxH)	43.18 x 80 x 4.45 cm (17 x 12 x 1.75 in)
Environmental	
Operating Temperature	10° to 50° Celsius (50° to 122° Farenheit)
Storage Temperature	-40° to 85° Celsius (-40° to 185° Farenheit)
Humidity	5% to 90% noncondensing
Electrical	
Power	Universal AC: single or dual 100-240 VAC, 50/60Hz, 1.4 A max Dual DC: 36 to 75 VDC, 5 A max
Safety and EMC Approvals and Markings	
Electromagnetic Emissions and Immunity	C-Tick, ICES 003 Issue 4 (February 2004), EN55022: 1998 + A1: 2000 + A2: 2003, EN55024: 1998 + A1: 2001 + A2: 2003, VCCI Class A, FCC Part 15 Class A
Safety	CAN/CSA-C22.2 No. 60950-1-03, EN60950-1:2001

CAUTION: To comply with FCC and CE certification requirements, use shielded cables when connecting target devices to the Ethernet ports. Failure to observe compliance requirements makes the equipment no longer compliant.

Appendix C: Target Device Configuration

This appendix provides details about target device configuration requirements that are unique to the MergePoint 5224/5240 SP manager.

During target device configuration, the administrator must assign parameters described in Table 4.16 on page 49 to each target device. This appendix provides information needed for configuring the following parameters:

- Target device type and command template
- A private subnet
- An optional virtual IP address, which hides the real IP address of the target device from users, and which requires the configuration of a virtual network (DNAT)

Configuring target device types and command templates

The MergePoint 5224/5240 SP manager uses the following four administrator-modifiable components described in this section for handling communications with target devices.

- Target device types
- Target device families
- Expect scripts
- Command templates

Target device types

Target device types are introduced in *Configuring new target device types* on page 49. Administrator-modifiable parameters that are defined for each target device type are the family and the command template, either or both of which can be modified to enable communications with target devices that do not work out of the box.

Target device families, Expect scripts, and command templates

Each target device family is defined by an Expect script in the /libeexec/spmanager directory in the form: talk_<family_name>.exp. For example, the Expect script that defines the iLO family is talk_ilo.exp.

The Expect scripts use text-based interfaces that are in command templates to log into the target devices and perform supported management actions on behalf of authorized users. One Expect script and one command template are assigned to each target device.

The default Expect scripts and command templates do not always work for all target devices of the same type because service processors of the same type often do not use the same syntax for their commands. For example, while power on is the command string that works to power on a server with some RSA II type service processors, power -on is the command string that works with some other RSA II type service processors. This section provides information about how administrators can test devices and create new or modified command templates, if needed to deal with command differences.

Defining families

To create a new device family, the administrator can create a customized Expect script by copying, renaming and modifying one of the default Expect scripts. The administrator should set the file permissions to allow reading and execution by all users and writing by members of the admin group. The format of a custom Expect script's file name should be: talk_customN.exp.

NOTE: New family names that adhere to the talk_<family_name>.exp format are visible to the cli command and to the DSView 3 software, but they are not visible in the Web Manager. For this reason, administrators need to create new Expect scripts for new families by using talk_custom1.exp, talk_custom2.exp, or talk_custom3.exp for the filenames.

Table C.1: Default Family Names and Corresponding Expect Script Names

Family Name	Expect Script Name
iLO	talk_ilo.exp
RSA II	talk_rsa_II.exp
DRAC	talk_drac.exp
IPMI 1.5	talk_ipmi_1.5.exp
IPMI 2.0	talk_ipmi_2.0.exp
ALOM	talk_alom.exp
DirectCommand	talk_DirectCommand_only.exp
devconsole	talk_devconsole.exp
custom1	talk_custom1.exp
custom2	talk_custom2.exp
custom3	talk_custom3.exp

SP/device Expect script arguments

With one exception, each of the Expect scripts used to control access to an SP takes exactly two arguments in the following format:

`talk_type.exp` *`servername action`*

The exception to the two-argument format occurs when the action is spconsole. When the second argument is spconsole, any other number of arguments may follow; all arguments entered after the spconsole action are collected into a single command to be executed in the target device's native command interface.

`talk_`*`type`***`.exp`** *`servername`* **`spconsole`** [*`command1`*|*`commandN`*]

servername

The servername is the alias configured for the server or device on the SP manager, for example, rsa_us. The script retrieves service processor/device specific information, such as the IP address, from the entry for the specified service processor/device, using the llconf program.

action

The action specifies the action for the script to take. The actions are listed below. Not all service processor/device types implement all of the listed actions. For example, the iLO type does not have a sensors reading feature, so the sensors action is not supported for iLO-type servers. See *SP/Device Expect script exit codes* on page 172 for the correct way to handle an unexpected action argument.

sensors

Asks the SP for a sensor reading and display service processor sensor output on standard output.

poweron

Asks the SP to power up its server.

poweroff

Asks the SP to power down its server.

powercycle

Asks the SP to reboot its server.

powerstatus

Asks the SP if its server is powered up.

reset

Asks the SP to reset its server.

sel

Asks the SP to retrieve the System Event Log and display the SEL contents on standard output.

clearsel

Asks the SP to clear the System Event Log.

spconsole

The native command line of the SP. Enters interactive pass-through mode. The script authenticates with the SP, then connects the SP output directly to its standard output and its standard input to the SP input.

NOTE: ssh must be invoked with the -t option when this mode is used.

devconsole

Enters a console (also known as Device Console) session on a server whose service processor supports console access to the server or enters a console session on a server or other device that supports device console access through its Ethernet port.

NOTE: ssh must be invoked with the -t option when this mode is used.

log_sensors

Retrieves sensor data in a standard format.

NOTE: ssh must be invoked with the -t option when this mode is used.

SP/Device Expect script exit codes

Scripts that handle devices must end with one of the exit codes shown in Table C.2.

Table C.2: Expect Script Exit Codes

Exit Code	Definition
0	Success
1	Unexpected output from service processor/device, or another error in an SP protocol (such as time-out)
2	Bad command line (such as an incorrect number of arguments)
3	Action argument is not valid for the SP/device type
4	Server or device given as first argument has not been configured

To create a custom Expect script:

1. Log into the SP manager console as an administrator.
2. Go to the /libexec/spmanager directory.
3. Copy an existing talk_<family_name>.exp and name the new file in the format: talk_customN.exp.

NOTE: Use talk_custom1.exp for the first custom script, talk_custom2.exp for a second, up to a total of three scripts.

4. Edit the script as desired.
5. Save and quit the file.
6. Make sure the permissions are still 755.

Contact your Avocent representative if you need additional support for creating a custom Expect script.

Command templates

Table C.3 lists the default command templates and describes the types of target devices to which they apply.

Table C.3: Default Command Templates

Template	Type of Target Device
alom.default	Sun ALOM type target devices
devconsole.default	Target devices that support access to their consoles.
drac.default	DRAC III/XT type target devices.
ilo.default	iLO type target devices.
ipmi_2.0.default	Not used.
rsa.default	Some RSA II type target devices.
rsa.limited.default	RSA II type target devices that support only power commands through their command line interface.
none	• IPMI 1.5 type target devices • Any type target device when only native IP access is being configured

All templates are listed in the Web Manager in the Config - Target devices Command template pull-down menu. If an administrator creates a new template, the new template automatically is added to the list the next time an administrative user logs into the Web Manager. An already-logged in administrative user can click the Cancel changes button to update the list.

Assigning a command template to a new target device

When adding a new target device that needs a template, the administrator must perform the following actions:

- Test whether the target device is compatible with the applicable default command template.
- If communications cannot be established with the new target device using a default command template, use the sptemplate utility to create and test a new command template, after making any needed changes to the commands that manage communications between the target device and the SP manager.
- If a new template cannot be made to work, create a custom Expect script to handle the target device’s requirements.

When one of the command templates is modified by an administrator, it applies to all target devices that use the template. Create a new template using the Web Manager when you do not wish to overwrite one of the defaults.

Using the sptemplate utility

An administrator (root or an administrative user) can use the sptemplate utility to test the default command templates when configuring a target device and to create a customized command template if needed.

A template can be configured to keep repeating commands to achieve a goal such as reading output from multiple classes of sensors on an RSA II target device or reading multiple event log files one by one until no more log files exist on an iLO-type service processor. Commands may be repeated until a string, such as No more entries, is returned. When commands are repeated, an escape sequence can be used to autoincrement the number in the command, which is needed, for example, when checking event log files.

The default editor used by sptemplate is vi. You can substitute nano for vi before invoking the sptemplate utility, as shown in the following screen example.

```
[root@MergePoint5224 /] export EDITOR=/bin/nano
```

After being invoked, the **sptemplate** utility displays the action menu shown in the following example.

```
[root@MergePoint5224 /] sptemplate
Please select action:


-View
 Edit
 New
 Copy
 Rename
 Delete
 Test
 Exit
```

Selecting *New* from the Action menu brings up an editor with a template file open for you to configure.

Selecting *View*, *Edit*, *Copy*, *Test* or *Rename* from the Action menu brings up a menu of templates like the one shown in the following screen example.

```
Please select template to view:

 drac.default
-rsa.default
 ilo.default
 rsa.limited.default
 alom.default
 ipmi_2.0.default
 devconsole.default
 none
 Exit
```

If *Test* is selected, after the administrator selects a template, a list of target devices that use the selected template appears, like the list shown in the following screen example.

```
Select Service Processor to test against:

-rack1_ibm_e360_rsa_II
 rack2_ibm_e360_rsa_II
```

After the administrator selects a template and a target device to test, a list of commands to test displays like the one shown in the following screen example.

```
Select a test to perform:

-Login and Native Command Interface
 Console Access
 Power On
 Power Status
 Power Cycle
 Reset
 Power Off
 System Event Log
 Clear Event Log
 Retrieve Sensors
 Test All
 Exit
```

Not all listed commands are supported on every type of target device. If you select an unsupported command, an error message displays that lists the supported commands.

The first time you select any action to test, you are prompted to enter a username and password. If local authentication is specified for the target device, enter the username and password that you entered to access the SP manager. If another authentication method is specified for the target device, use the appropriate username and password for the specified authentication method. The test command uses the same authentication and authorization processes that the SP manager uses in its normal operation, as explained in *MergePoint 5224/5240 SP Manager Authentication Options* on page 22 and *User and Group Configuration* on page 25.

See the following examples:

- The MergePoint 5224/5240 SP manager uses local authentication, and the administrator logs into the SP manager using the spmanager username and password pair: root/root_password.
- The administrator tests the rsa.default command template on a server called rack1_ibm_e306_rsa, which is configured for RADIUS authentication with username scottb and password cycl123. The administrator must enter scottb and cycl123 to perform the test.
- The administrator tests the rsa.default command template on a server called rack2_ibm_e306_rsa, which is configured for LDAP authentication with username sburns and password 123cycl. The administrator must enter sburns and 123cyclto perform the test.
- The administrator tests the rsa.default command template on a server called rack3_ibm_e306_rsa, which is configured for local authentication. The administrator must

enter the same username/password pair that was entered to access the SP manager (root/root_password.) to perform the test.

Each set of commands may be tested in any order after the login test is performed. Errors are generated if a command is entered out of logical order; for example, if the Reset command is issued for a server that is not powered on. After any test you can return to the editor to make changes.

While using the editor to edit, copy or create a new template, you can edit or delete fields and add comments. When the file is saved, error checking is performed. If an error is found, you are prompted either to enter the editor again to fix the error, or to discard the changes.

The following are examples of commands

```
login_prompt = ogin:
pass_prompt = sword:
cmd_prompt = [[][^]]+[]]#
logout_cmd = exit
poweron_cmd = serveraction powerup
poweroff_cmd = serveraction powerdown
powercycle_cmd = serveraction powercycle
powerstatus_cmd = {
       mapcase = lower
       inmap = %d %s %s %s %s %s %s
       outmap = Powerstatus: %5$s
       command = getmodinfo
  }
reset_cmd = serveraction hardreset
sel_cmd = {
     inmap = %d %d-%[a-z]-%d %d:%d:%d %[^^M]
     outmap = %1$d||%2$d/%3$s/%4$d|%5$d:%6$d|%8$s
       command = getsel
  }
clearsel_cmd = {
     command = racadm clrsel
      write = Succeeded.\n
  }
devconsole_cmd = connect com2
  devconsole_esc = \r~.
```

You cannot change templates whose name ends with the .default suffix. sptemplate warns about this restriction if you try to edit or rename these templates, and it requests confirmation before allowing you to create a new template with a .default suffix through the New, Rename or Copy functions.

To find out if an existing command template works with a new target device:

1. Assign the target device the appropriate device type and the associated default command template for the device type.
2. Try to run power management commands on the target device.
3. If the target device is an RSA II type device, if you cannot run power commands on the target device using the rsa.default template, assign the target device the rsa.limited.default template.
4. If you can run power commands on the target device, test the rest of the management commands that are supported on the device type. If they work, you are done.
5. If you cannot run one or more of the supported commands on the target device, attempt to connect to the SP console.

NOTE: Even if the power management commands do not work on a new target device, you can usually establish a connection to the SP's console.

6. If you cannot access the SP console, perform the following steps:
   a. Use **ping**, **telnet** or **ssh** to verify that you can get to the server.
   b. If you cannot access the server, check the network configuration and fix the problem that is preventing access.
7. If you can access the server but still cannot access the SP's console, double-check the username and password you are using against the username and password that are configured for the target device.
8. Once you have established the connection to the SP's console, type the help command, which gives you the syntax you need to use for the commands supported by the SP.
9. Note the syntax of the commands supported by the SP's console, and go to the next procedure.

To use the sptemplate utility to create a new template:

Perform this procedure after *To find out if an existing command template works with a new target device:* on page 178, if the default templates do not work for a new target device.

NOTE: If you select *Config - Target device type* in the Web Manager and select the *Configure target device templates* button, you are logged into the console and the sptemplate utility automatically launches, so you can go directly to Step 2

1. Log into the console as an administrator and run the **sptemplate** utility.
2. Select *New* from the menu.
3. Enter a name, such as rsa.new. The editor brings up a template for a new command template and assigns it the name you specified.

a. Modify the prompts and commands as needed, using the syntax supported on the target device. Sensors may not be supported. If any command is not supported, leave it commented out in the template.

CAUTION: You must specify the escape sequence used by the device's console. It is captured by the SP manager and it is used to log the user out of the SP console whenever the user logs out of the device console, preventing unauthorized access to the SP console.

4. Save and quit the file.
5. Enter the **saveconf** command.
6. Log out from the console.
7. Log into the Web Manager as an administrative user and select the *Config - Target devices* menu option.

   When an administrative user logs in, the new template is automatically added and is included in the list of command templates that you can assign to a target device.
8. Assign the new template to the target device.

To use the sptemplate utility to test a template:

When sptemplate is used to test a template, extra debugging information is provided to report on commands sent to and received from the target device.

1. Log into the console as an administrator and invoke the **sptemplate** utility.
2. Select *Test* from the menu.
3. At the prompt, confirm that you want to continue by entering **y**. A list of templates appears.
4. Select a template to test. A list of configured target devices appears.
5. Select a target device to test the template against. The editor runs the commands in the specified template and returns debugging information that you can record for making command changes in a new template.
6. Choose a command to test.
7. At the prompt, enter the username and password you used when logging into the SP manager.
8. Go to *To use the sptemplate utility to create a new template:* on page 178.

Address configuration for target devices

Table C.4 lists related topics the administrator must understand when planning and implementing the private IP addresses and provides links to where they are documented.

Table C.4: Tasks for Creating Addresses to Assign to Target Devices

Task	Where Described
Private IP addresses must be defined by the creation of at least one *private subnet.* A private subnet must be created for each IP address range used by the target devices.	• *Why define private subnets?* on page 182 • *Configuring a private subnet* on page 183 • *Example 1: Private subnet configuration* on page 184 • *Example 2: Two private subnets and VPN configuration* on page 185
Private subnet(s) should use IP addresses from one of the three IP address ranges reserved for use on internal networks.	• *Using reserved IP addresses for private IP addressing* on page 181
Even if virtual IP addresses are used (as described below), the planned real IP address for each target device must be either configured manually as a static IP address or configured as a fixed address in the DHCP server dhcp.conf configuration file.	• *Options for assigning IP addresses to target devices* on page 198
A *virtual network* may be created in the following cases: • To hide a target device's private IP addresses from non-administrative users who are not configured for native IP access. • When it is desired that multiple non-contiguous private subnets be supported by a single network route (or, in the case of IPSec, a single tunnel) on the client for VPN or native IP access. This would be the case when target devices are already configured using IP addresses from multiple address ranges and it is not feasible to change previously defined target device IP addresses.	• *Why define virtual (DNAT) addresses?* on page 192 • To Configure IP Addresses From Multiple Ranges • *Example 3: Virtual network with two private subnets and VPN configuration* on page 193

Table C.4: Tasks for Creating Addresses to Assign to Target Devices (Continued)

Task	Where Described
Any user who needs native IP access to the SP manager must create a named VPN connection profile, then to create a VPN tunnel to the SP manager before enabling native IP. The requirements for creating the VPN tunnel and the IP addresses to use vary depending on whether IPSec or PPTP is being used.	• *Routing requirements for native IP access* on page 184 • *IPSec VPN configuration for example 2* on page 188 • *PPTP VPN configuration for example 2* on page 189 • *Enabling native IP and accessing a target device's native features using real IP addresses for example 2* on page 191 • *IPSec VPN configuration for example 3* on page 195 • *PPTP VPN configuration for example 3* on page 196 • *Enabling native IP and accessing a target device's native features using virtual network addresses for example 3* on page 197

Using reserved IP addresses for private IP addressing

The administrator should assign a private IP address to each target device from one of the three IP Internet address ranges that are reserved for use on internal networks. Table C.5 shows the reserved IP address ranges for internal networks.

Table C.5: IP Address Ranges Reserved for Internal Network Addressing

Address Range	# of Networks/Class	Network Sizes
192.168.0.0—192.168.255.255	256/Class C	small (fewer than 200 hosts)
172.16.0.0—172.31.255.255	16/Class B	mid-sized
10.0.0.0—10.255.255.255	1/Class A	large

See http://www.rhebus.com/techinfo/iprange.htm#ip1 for recommendations about which ranges to use for various sizes of organizations and for avoiding address conflicts.

The number of IP addresses available on a network may be restricted by a subnet mask. For a simple example, the subnet mask 255.255.255.0 provides 256 IP addresses. The IP address ending with zero (0) is the network address, and the IP address ending with 255 is the broadcast address, leaving 254 addresses to assign to target devices (from 1-254).

To specify a range of addresses on the MergePoint 5224/5240 Service Processor Manager supply the network address and a subnet mask, in either of these two formats: 192.168.0.0 and 255.255.255.0 or 192.168.0.0/24.

Why define private subnets?

At least one private subnet must be defined on the SP manager for the following purposes:

- To define a private address for the SP manager and target devices to use when communicating.
- To enable communications between remote user's workstations on the Internet or local user's on the same LAN and target devices on the private management network, via the SP manager's native IP access facility.

The private Ethernet ports are accessed through the priv0 interface on the SP manager, which interacts with target devices through an internal switch.

The SP manager attempts to reach a target device that does not have a private subnet assigned by attempting to contact it through the SP manager's default route. Therefore, unless the administrator defines a private subnet and assigns it to each target device, the target device cannot be reached unless the target device is on the public side of the SP manager. In almost all cases, target devices are on the private side of the SP manager and therefore they are unreachable without a private subnet.

The following should be kept in mind when planning the addressing scheme:

- When the target devices' addresses are all within the same range, only one private subnet is required.
- The administrator should assign IP addresses to all service processors from the same block of addresses, if possible, to make it possible to administer the IP addresses using only a single private subnet.
- When the target devices' addresses are already configured in multiple ranges and the addresses cannot be changed, or when for some other reason, target devices must have addresses in multiple address ranges, multiple private subnets must be created. (To simplify routing for PPTP VPN connections, multiple private subnets may also require configuration of a virtual network, as described in *Why define virtual (DNAT) addresses?* on page 192.)
- The priv0 interface, which is used for all the private Ethernet ports, is not assigned an IP address unless a private subnet is configured.

The following screen example shows the default ifconfig output for priv0, which shows no IP address.

```
priv0    Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
         UP BROADCAST RUNNING MULTICAST   MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:100
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
         Base address:0xe000
```

The administrator must define either an IP address or addresses for priv0 by defining private subnet(s). When multiple private subnets exist, their IP addresses are assigned to aliases of priv0, such as priv0:sub1 and priv0:sub2.

Configuring a private subnet

An administrator configures a private subnet by performing the following:

- Defining a range of IP addresses which administrators can assign to target devices that are connected to the private ports.
- Designating one of the IP addresses within the specified range to be used by the SP manager. The appliance-side address must be used by users when creating a IPSec VPN connection to enable native IP access.

The SP manager uses the specified information to create a route to the private subnet.

The range of IP addresses is derived from the information shown in Table C.6, which the administrator supplies to define a private subnet.

Table C.6: Values for Configuring a Private Subnet

Field	Definition
Private subnet name	Any meaningful name chosen by the administrator, such as privnet1.
Appliance side IP address	Target devices use this address when communicating with the SP manager. The SP manager uses this address when communicating with target devices. This address must be within the private subnet's IP address range.
Subnet mask	Defines the range of addresses available on the private subnet.

The system derives the range of addresses that can be used for talking to target devices by using the network portion of the SP manager's IP address and from the private subnet netmask that the administrator specified.

When configuring a target device, the administrator assigns the private subnet to the target device and assigns an IP address within the range specified for the private subnet. The SP manager uses the target device's IP address when talking to a target device, and target devices use the SP manager's assigned address when talking the SP manager.

When a private subnet is configured, the private subnet name is assigned to the priv0 interface in the form priv0:private_subnet-name along with the IP address assigned to the SP manager in the form inet addr: <SPmanager_IPaddress>. If multiple private subnets are configured, multiple priv0:private_subnet-name interfaces exist, each with its administratively configured private subnet IP address for the SP manager. See the following examples for sample ifconfig output:

- *Example 1: Private subnet configuration* on page 184
- *Example 2: Two private subnets and VPN configuration* on page 185

Routing requirements for native IP access

As documented in the MergePoint 5224/5240 Service Processor Manager User Guide, users who are authorized for native IP access need to create a IPSec or PPTP VPN connection before gaining native IP access.

Any routes needed for IPSec VPN can be configured as part of the IPSec connection by setting the nexthop to the IP address of the desired network or host route and setting the boot action to Add and route.

Any route(s) needed for PPTP must be configured manually.

See *IPSec VPN configuration for example 2* on page 188, *PPTP VPN configuration for example 2* on page 189, *IPSec VPN configuration for example 3* on page 195 and *PPTP VPN configuration for example 3* on page 196, which discuss routing requirements for the two types of VPN connections and show example routes.

Example 1: Private subnet configuration

Figure C.1 shows a private subnet configuration example.

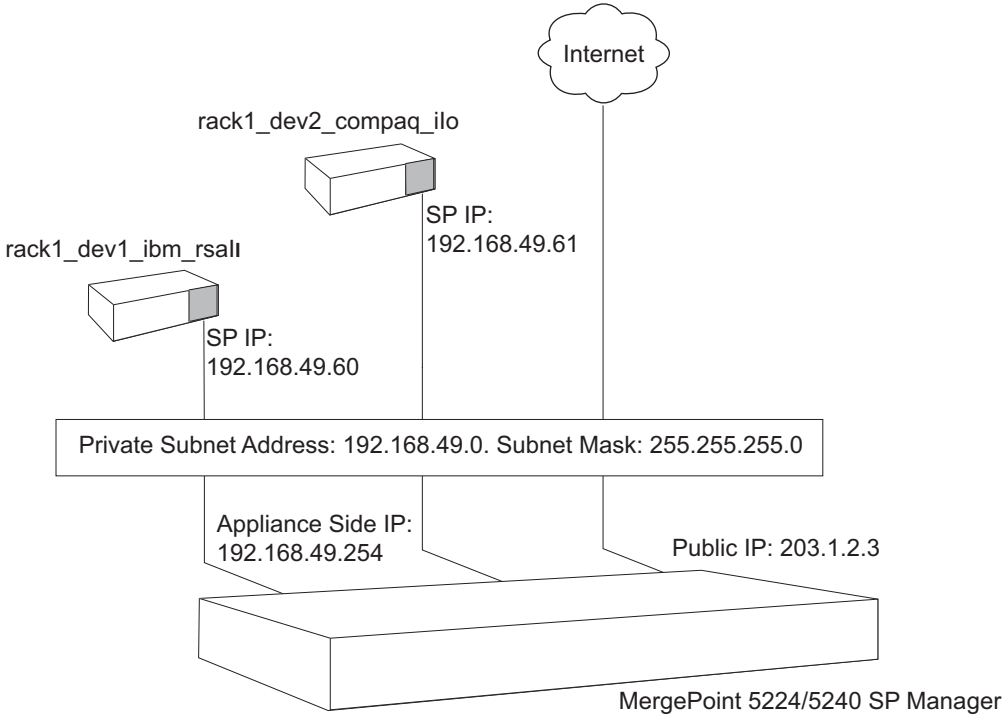

Figure C.1: Example 1: Private Subnet

In Figure C.1, two devices are connected to the SP manager. The public Ethernet port has a public IP address of 203.1.2.3. The administrator plans to assign the following:

- Two private IP addresses within the 192.168.49.0 network range to the devices on the SP manager's private network: 192.168.49.60 and 192.168.49.61
- A third private IP address within the same range to the SP manager: 192.168.49.254

The following values would be entered in the dialog that appears when the Add Subnet button is clicked on the Network - Private subnets screen:

- Private subnet name: privnet
- Appliance side IP address: 192.168.49.254
- Subnet netmask: 255.255.255.0.

The private subnet address derived from the configuration is 192.168.49.0. For this network IP address, the conventional broadcast address is 192.168.49.255. Because the appliance side address is 192.168.49.254, the administrator can assign any remaining IP address between 192.168.49.1 and 192.168.49.253 when configuring a target device.

These values: Private subnet privnet and Target device IP address 192.168.49.61 assigned to the device rack1_dev2_compaq_ilo on the Web Manager - Config Target devices screen. As shown in the following example, the new private subnet name and the appliance-side IP address and subnet mask fare assigned to the priv0 interface.

```
priv0:privnet Link encap:Ethernet HWaddr 00:60:2E:BB:AA:AA
          inet addr:192.168.49.254  Bcast:192.168.49.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Base address:0xe000
```

Example 2: Two private subnets and VPN configuration

Figure C.2 shows an example with four devices. Two subnets must be created because the devices sp3 and sp4 have IP addresses that cannot be changed, and their addresses are not in the same network range as the other two devices. Configuration details follow, including how to set up VPN connections.

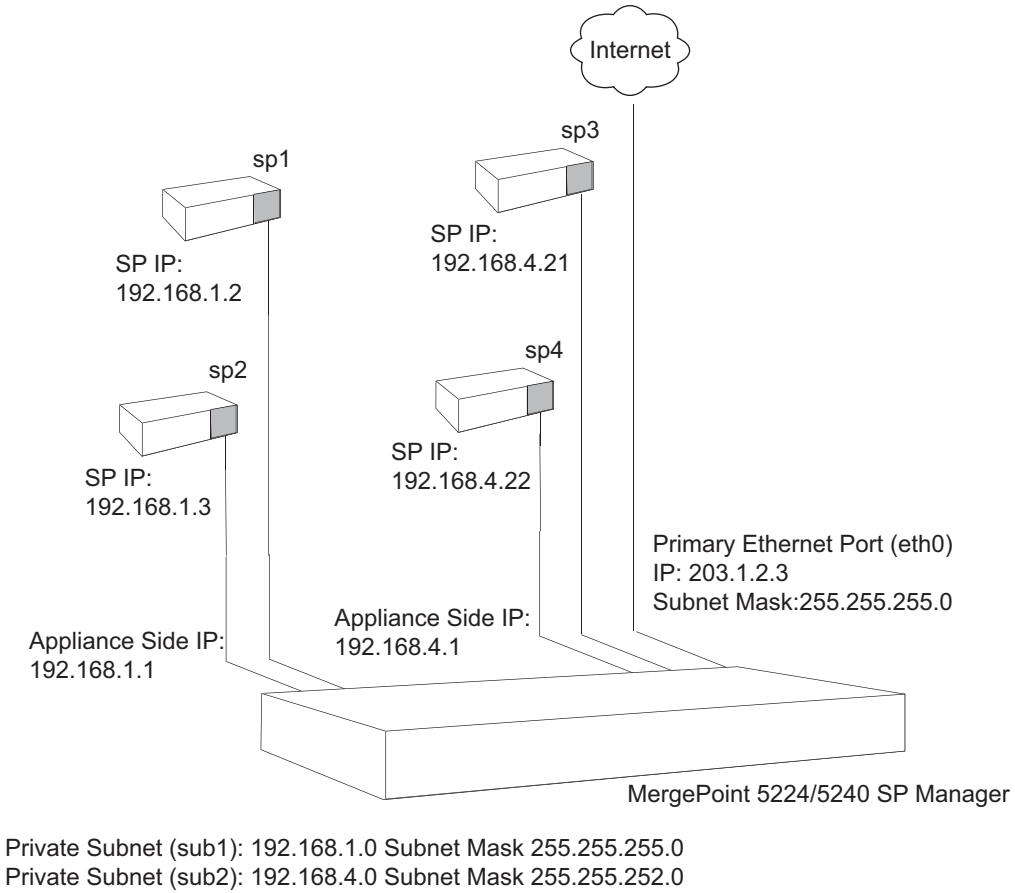

Figure C.2: Example 2: Two Private Subnets

Two private subnets and user configuration for example 2

Configuration of the private subnets shown in Figure C.2 is described in the following bulleted list:

- The primary Ethernet port is configured with IP address 203.1.2.3 and subnet mask 255.255.255.0.
- A default route is automatically created using a gateway IP 203.1.2.254, which the administrator assigned when configuring the primary Ethernet port.
- Private subnets are configured as aliases to priv0 by defining the appliance side IP addresses and netmasks shown in Figure C.2 and listed below:
  - Private subnet sub1
  - Appliance side IP address: 192.168.1.1

- Subnet mask: 255.255.255.0

The above values define a range between 197.168.1.0 and 192.168.1.255 = 256 addresses, of which 254 are usable.

- Private subnet sub2
- Appliance side IP address: 192.168.4.1
- Subnet mask: 255.255.252.0

The above values define a range between 197.168.4.0 and 192.168.7.255 = 1054 addresses, of which 1022 are usable. This subnet is defined with this address range because target devices sp3 and sp4 have previously been assigned IP addresses within this range, and the addresses cannot be changed.

As shown in the example output from the ifconfig command below, both private subnet names are assigned as aliases to the priv0 interface and the appliance-side IP addresses and subnet masks are assigned to each alias.

```
priv0:sub1 Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
          inet addr:192.168.1.1  Bcast:192.168.0.255
          Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Base address:0xe000
priv0:sub2 Link encap:Ethernet  HWaddr 00:60:2E:BB:AA:AA
          inet addr:192.168.4.1  Bcast:172.10.0.255
          Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Base address:0xe000
```

The configuration of the target devices shown in Figure C.2 is described in the following bulleted list:

- sp1 is on private subnet sub1, so it needs an IP address in the range 192.168.1-192.168.1.255: 192.168.1.2.
- sp2 is also on private subnet sub1, so its IP address in the same range: 192.168.1.3.
- sp3 is on private subnet sub2. It has previously been assigned the IP address 192.168.4.21, which cannot be changed.
- sp4 is also on private subnet sub2. It has previously been assigned IP address 192.168.4.22 and its address cannot be changed either.

To configure the user to be able to create the VPN tunnel, an administrator must make sure that the user who needs the VPN access is authorized for native IP access to the devices.

IPSec VPN configuration for example 2

After the private subnets, target device and user account configuration in *Two private subnets and user configuration for example 2* on page 186 is completed, a VPN connection must be created. This example shows the configuration steps that must be performed by the administrator and by a user on a remote workstation for enabling two IPSec VPN connections. One connection supports the IPSec VPN tunnel from the user's workstation to sp1 and sp2. The second connection supports the IPSec VPN tunnel to sp3 and sp4.

The administrator must also perform the following actions to enable an IPSec client to access the private subnets where the target devices reside:

- Make sure that the IPSec service is enabled on the SP manager.
- Obtain the IP address of the user's workstation and use it to create two named IPSec connections (connSub1 and connSub2) with the following values specified:
    - Left ID: @mergepoint5224
    - Left IP address: 203.1.2.3 (must be one of the SP manager's public IP addresses)
    - Left nexthop: leave blank if the user's workstation and the SP manager are able to exchange packets.

NOTE: The user can test whether the user's workstation can access the SP manager by entering the SP manager's public IP address in a browser to try to bring up the Web Manager.

    - When configuring connSub1 for access to sub1: Left subnet: 192.168.1.0/24
    - When configuring connSub2 for access to sub2: Left subnet: 192.168.4.0/22
    - Right ID: @workstation
    - Right IP address: the IP address of the user's workstation: 12.34.56.78
    - Right nexthop: leave blank if the user's workstation and the SP manager are able to exchange packets
    - Right subnet: leave blank

The other IPSec configuration parameters (such as Authentication protocol and Boot action) would be determined by the site's policy, equipment compatibility and site routing requirements.

NOTE: In some circumstances (for example, if packets are being blocked by a firewall on the client's default gateway), the user's workstation and the SP manager are not going to be able to exchange packets. Setting one or both of the Right and Left nexthop parameters to the IP address of a host route and selecting Add and route as the boot action may be needed to create a route that allows the two endpoints to communicate.

In addition, the administrator must perform the following actions to enable the IPSec client to access the subnets where the target devices reside:

- Give the user a copy of the parameters used to configure the IPSec connection profiles on the SP manager.

The administrator can send a copy of the relevant portions of the ipsec.conf file after the changes are saved and applied in the Web Manager for the user to insert into the ipsec.conf file on the user's workstation.

The authorized user must perform the following to actions enable the IPSec client running on the user's workstation to bring up the VPN tunnel to access the subnets where the target devices reside and then to access the native IP features on the target devices.

- Use the same values used by the administrator to create an IPSec VPN connection profile on the user's workstation.

  If the administrator sends the relevant portions of the ipsec.conf file from the SP manager's IPSec configuration, use it to replace the same section in the workstation's ipsec.conf file.
- Bring up the IPSec VPN tunnel.

  Depending on the platform and IPSec client being used, the user may use a GUI or execute the ipsec auto -up command. IPSec automatically creates the routes needed to get packets flowing through the tunnel, so neither the user nor the administrator need to create routes to support IPSec access to target devices.
- Enable native IP and access the target device's native features.

  See *Enabling native IP and accessing a target device's native features using real IP addresses for example 2* on page 191.

PPTP VPN configuration for example 2

After the private subnets, target device and user account configuration in *Two private subnets and user configuration for example 2* on page 186 is completed, a VPN connection must be created. This example describes the configuration steps that must be performed by the SP manager administrator and by a user on a remote workstation for setting up an PPTP VPN connection that would enable the authorized user allSps to access sp1, sp2, sp3 and sp4.

The MergePoint 5224/5240 SP manager's administrator must perform the following to enable the PPTP client:

- Make sure that the PPTP service is enabled.
- Configure PPTP on the SP manager.

Following are two example address pools:

- PPTP local address pool: 192.168.2.1-10
- PPTP remote address pool: 192.168.3.1-10

NOTE: The address pools' IP addresses can be assigned arbitrarily. Make sure that none of the addresses assigned here are being used elsewhere on your network.

Make sure the following are done for the user who needs the PPTP VPN access:

- The user's account is authorized for native IP access to sp1, sp2, sp3, and sp4.
- The user's account is configured for PPTP access to the SP manager.

NOTE: The user can be configured for PPTP alone or for both PPP/PPTP.

- The user's workstation is running PPTP client software.
- The user has the PPTP password if it is different from the password that authenticates the user for access to the SP manager.

The authorized user must perform the following configuration:

- Make sure the user's workstation can exchange packets with the SP manager.

  The user can test whether the user's workstation can access the SP manager by entering the SP manager's public IP address in a browser to try to bring up the Web Manager.
- If a network or host route is needed to enable communications with the SP manager, configure the route.
- Use the PPTP client on the workstation to create the PPTP VPN connection profile, entering the following:
  - PPTP server address = SP manager public IP address (203.1.2.3)
  - Username = SP manager username, in this example: allSPs
  - Password = PPTP password
- Create the PPTP VPN connection.
- Enter the ifconfig or ipconfig command on the command line of the user's workstation to discover the IP address assigned to the SP manager's end of the PPTP VPN tunnel.

  When the PPTP tunnel is being activated, the SP manager chooses an IP address from each of the address pools for the endpoints of the PPTP link. The client's end of the point-to-point link receives an address from the remote address pool, and the SP manager receives an address from the local address pool. Usually the first connection obtains the first address from each pool, so the client would be 192.168.3.1 and the SP manager would be 192.168.2.1.
- Enter the SP manager's PPTP-assigned address either in a browser or with ssh on the command line to access the SP manager. In this example the address would be 192.168.2.1.
- Create a static route to inform the workstation that the target devices to be contacted are at the other end of the point-to-point link.
- In this example, to communicate with sp1 and sp2, a route would needed to sub1, which has the network IP address 192.168.1.0 as shown below:

  ```
  route add -net 192.168.1.0 mask 255.255.255.0 via 192.168.2.1
  ```

- To communicate with sp3 and sp4, a route would needed to sub2, which has the network IP address 192.168.4.0 as shown below:

  ```
  route add -net 192.168.4.0 mask 255.255.255.0 via 192.168.2.1
  ```

- Enable native IP and access the target device's native features.

Enabling native IP and accessing a target device's native features using real IP addresses for example 2

After creating the VPN tunnel as described in *IPSec VPN configuration for example 2* on page 188 or *PPTP VPN configuration for example 2* on page 189, the user uses the appliance side IP address configured for the appropriate private subnet to access the SP manager and then enables native IP access to the desired target device.

Enabling native IP access

In this example, to enable native IP access on sp1 or sp2 on sub1, the user would enter the appliance side IP address for sub1 (which is 192.168.1.1) in one of the two following ways:

- In a browser on the user's workstation, the user would perform the following actions:
  - Bring up the Web Manager using http://192.168.1.1.
  - Select the *Target devices* left menu option.
  - Select *sp1* or *sp2*.
  - Click *Enable Native IP*.
- On the user's workstation's command line, the user would perform the following actions:
  - Use SSH to connect to the SP manager's console and to access the rmenush menu. Select *Access Devices* from the menu.
  - Select either *sp1* or *sp2*.
  - Select *Enable native IP* from the list of management actions the user is authorized to perform on the target device.

    -or-
  - Enter **ssh** to execute the **nativeipon** command directly using the target device alias

Accessing native features for example 2

After enabling native IP access, the user can access one of the desired native features that may be available on the target device, including a native web application or a native management application.

A native web application may be accessed in one of the following ways:

- In the Web Manager on the SP manager, the user selects the *Go to native web interface* link on the Access Target Devices screen.
- On the user's workstation, the user enters either the IP address or DNS-resolvable name of the target device in a browser.
- On the user's workstation, the user enters the **ssh** command with the name/alias of the target device along with the IP address of the appliance side address for the subnet where the target device resides.

A native management application may be accessed in one of the following ways, depending whether the application is a client on the user's workstation or resides on the SP:

- If the management application resides on the user's workstation, the user brings up the management application from the workstation.
- If the management application resides on the SP, and is an executable that can be invoked on the command line, the user accesses the SP's console first in one of the following two ways:
  - The user enters **ssh** with the **spconsole** command.

    -or-
  - In the Web Manager on the SP manager, the user selects *Access -Target Devices* and selects the *SP Console* menu option.

  The user then brings the management application up from the SP's command line.

Why define virtual (DNAT) addresses?

A virtual network based on DNAT may be defined in the following cases:

- To hide the addresses of the target devices from users by the use of virtual IP addresses.

CAUTION: When an authorized user has service processor access, target device console access or native IP access, there is no way to prevent that user from seeing the IP address of the target device while the user is connected.

  It is possible and desirable to hide target devices' real IP addresses from users who are authorized to access all other device management capabilities other than native IP, service processor console or device console.
- When multiple private subnets must be supported by a single network route, and you do not want to require authorized users to configure routes to each network.

  For example, if three target devices have addresses 192.168.0.1, 10.0.25 and 17.10.11.12, three private subnets could be defined. A virtual network would map the IP addresses from the three private subnets to virtual IP addresses in the same virtual network range.

Table C.7 describes the information that defines a virtual network.

Table C.7: Information Defining a Virtual (DNAT) Network

Field	Description
Address	IP address to assign to the SP manager from the virtual network address range. For example, if the virtual IP address of the network is 10.0.0.0, 10.0.0.254 would be a valid IP address that could be assigned to the SP manager. The administrator would then have all the other addresses to assign to target device, except for 10.0.0.0 and 10.0.0.255.
Netmask	Netmask is used in combination with the network address portion of the Address above to define the address range of the virtual network.

NOTE: Some service processors do not work with virtual network (DNAT) addresses.

Example 3: Virtual network with two private subnets and VPN configuration

This example adds to the configuration of two private subnets with four target devices by configuring a virtual network, which has the following benefits:

- It simplifies routing for PPTP VPN users.
- It hides IP addresses from users who are authorized only for one of the following types of device management actions:
    - Power commands
    - Sensor commands
    - System event log commands

The following figure shows the same configuration as Figure C.2, but with the addition of virtual IP addresses.

Figure C.3 shows an example of virtual network configuration that enables virtual addresses to be assigned to target devices and to the SP manager. The administrator plans to assign virtual IP addresses in the 172.20.0.1 range to hide the real private subnet IP addresses.

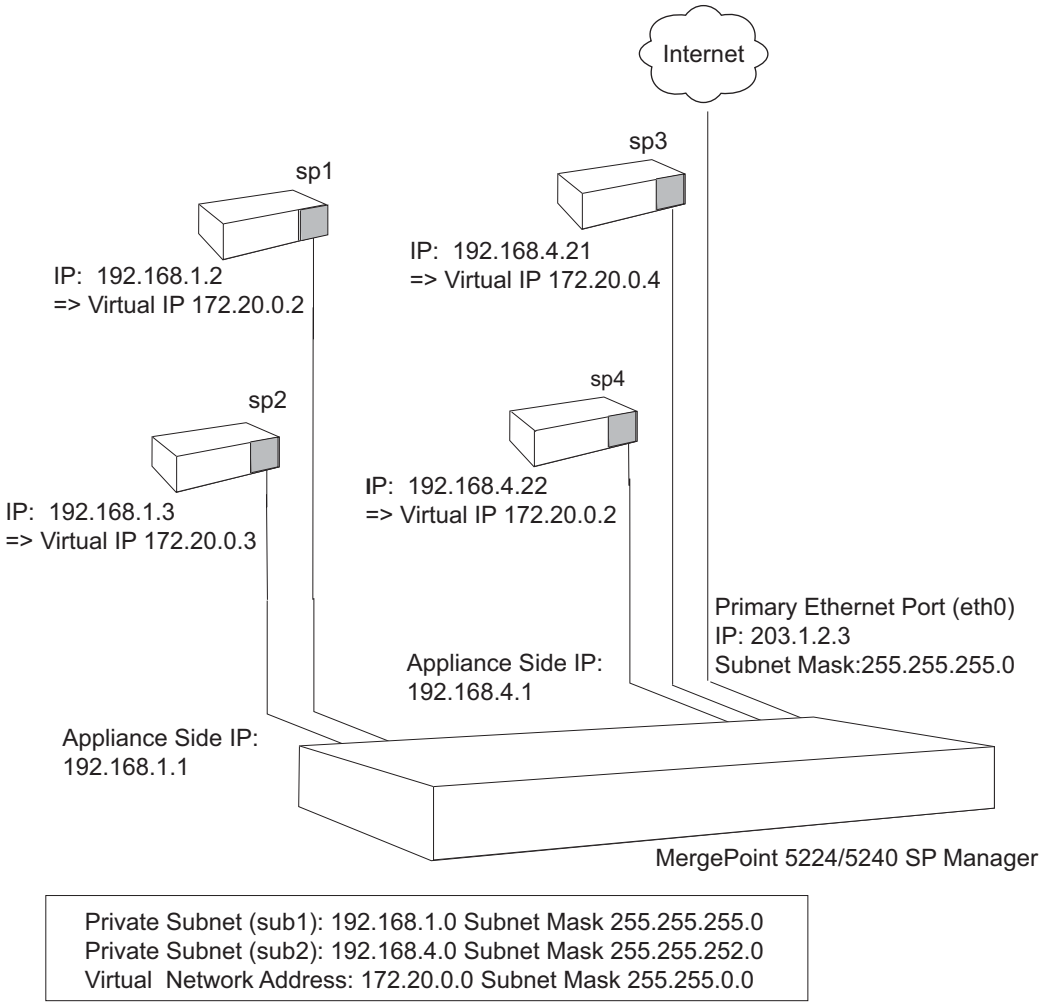

Figure C.3: Example 3: Virtual Network Configuration

NOTE: sp4 in Figure C.3 is an SP that does not work with virtual network (DNAT) addresses.

Virtual network and target device configuration for example 3

To hide the real addresses of the target devices from users according to the ongoing example, the administrator would need to perform the following additional configuration:

- Assign the target device named sp1 a virtual IP of 172.20.0.2.
- Assign the target device named sp2 a virtual IP of 172.20.0.3.
- Assign the target device named sp3 a virtual IP of 172.20.0.4.

- The target device named sp4 with IP 192.168.4.22 does not work with virtual network (DNAT) addressing, so it cannot be contacted using a virtual IP address. Therefore, the administrator does not assign sp4 a virtual IP.

To make it possible to assign the virtual addresses shown in Figure C.3, the SP manager's administrator must configure a virtual network with the following values:

- Address: A virtual address from the desired virtual address range to assign to the SP manager, in this case: 172.20.0.1
- Netmask: 255.255.0.0

Finally, the administrator also must configure the target devices that support virtual addressing with a virtual address from the 172.20.0.0 virtual network IP range. In this example, virtual IP address 172.20.0.2 is assigned to the target device sp1 on the Web Manager Config Target Devices screen to implement the configuration. On the Target Devices screen, the IP addresses for sp1, sp2, and sp3 are hidden, and the user can only see the target devices' virtual IP addresses. Because sp4 does not work with virtual IPs and no virtual IP was configured for sp4, the user sees sp4's real IP address.

IPSec VPN configuration for example 3

After the private subnets, target device and user account configuration in *Virtual network and target device configuration for example 3* on page 194 is completed, a VPN connection must be created. With a virtual network, only one IPSec VPN connection must be configured to create the IPSec VPN tunnel from the user's workstation to sp1, sp2 and sp3, which are on both private subnets in example 3.

Configuration of connSub2 would be still be needed as in *IPSec VPN configuration for example 2* on page 188, because the only way a user could contact sp4 would be through the private subnet IP.

The values used for enabling an IPSec VPN connection are the same as in *IPSec VPN configuration for example 2* on page 188, except the SP manager's administrator must configure the Left subnet: by entering 172.20.4.0/22 to configure the connection to the virtual network.

As in the earlier example, the administrator must perform the following actions to enable the IPSec client to access the subnets where the target devices reside:

- Give the user a copy of the parameters used to configure the IPSec connection profiles on the SP manager.

  The administrator can send a copy of the relevant portions of the ipsec.conf file after the changes are saved and applied in the Web Manager for the user to insert into the ipsec.conf file on the user's workstation.

The authorized user must perform the following configuration to enable the IPSec client running on the user's workstation to bring up the VPN tunnel to access the subnets where the target devices reside and then to access the native IP features on the target devices.

- Use the same values used by the SP manager's administrator to create an IPSec VPN connection profile on the user's workstation.

If the SP manager's administrator sends the relevant portions of the ipsec.conf file from the appliance's IPSec configuration, use it to replace the same section in the workstation's ipsec.conf file.

- Bring up the IPSec VPN tunnel. For accessing sp1, sp2 or sp3, the user can use the connVirt connection profile. For accessing sp4, the user uses the connSub2 connection profile.

Enabling native IP and accessing the target device's native features is the same as described under *Enabling native IP and accessing a target device's native features using real IP addresses for example 2* on page 191.

PPTP VPN configuration for example 3

After the private subnets, target device and user account configuration in *Virtual network and target device configuration for example 3* on page 194 is completed, a VPN connection profile must be defined to create a VPN tunnel to the virtual network.

The steps used for enabling a PPTP VPN connection to the virtual network are the same as in *PPTP VPN configuration for example 2* on page 189, except that, after creating the PPTP VPN tunnel, the user must create the static route differently to access the virtual network.

This first set of bullets are a review of the steps for obtaining the PPTP address assigned to the SP manager:

- Enter the ifconfig or ipconfig command on the command line of the user's workstation to discover the IP address assigned to the SP manager's end of the PPTP VPN tunnel.
- Enter the SP manager's PPTP-assigned address either in a browser or with ssh on the command line to access the SP manager. In this example the address is 192.168.2.1.

The next bulleted items show how to create an appropriate route to the virtual network.

- Create a static route to inform the workstation that the target devices to be contacted are at the other end of the point-to-point link.

  In this example, to communicate with sp1, sp2 and sp3, a route would needed to the virtual network whose IP address is 172.20.0.0 as shown below:

  ```
  route add -net 172.20.0.0 mask 255.255.0.0 via 192.168.2.1
  ```

  To communicate with sp4, because it cannot be contacted through a virtual network IP address, the same route mentioned in *PPTP VPN configuration for example 2* on page 189 would be needed to sub2, which has the network IP address 192.168.4.1 as shown below:

  ```
  route add -net 192.168.4.1 mask 255.255.252.0 via 192.168.2.1
  ```

- Enable native IP and access the target device's native features.

Enabling native IP and accessing the target device's native features is the same as described under *Enabling native IP and accessing a target device's native features using real IP addresses for example 2* on page 191.

Enabling native IP and accessing a target device's native features using virtual network addresses for example 3

After creating the VPN tunnel as described in *IPSec VPN configuration for example 3* on page 195 or *PPTP VPN configuration for example 3* on page 196, the user enables native IP and accesses a target device's native features.

In this example, to access sp4, which is a type of service processor that does not work with virtual network addresses because it is not compatible with DNAT, the user would enter the SP manager's real address, as described in *Enabling native IP and accessing a target device's native features using real IP addresses for example 2* on page 191.

Enabling native IP access for example 3

In this example, to enable native IP access to sp1, sp2, or sp3, the user would enter the SP manager's virtual IP address, which is 172.20.0.1, in one of the two following ways:

- In a browser on the user's workstation, the user would perform the following actions:
  - Bring up the Web Manager by entering the **http://172.20.0.1** URL.
  - Select the *Access - Target Devices* left menu option.
  - For either sp1, sp2 or sp3, click *Enable Native IP access*.
- On the user's workstation's command line, the user would perform the following:
  - Enter **ssh** to connect to the SP manager's console and to access the rmenush menu in one of the following ways:

    ssh *username*:**@172.20.0.1**

    -or-

    ssh -t *username*:**@172.20.0.1 menu**
  - Select *Access Target Devices* from the menu.
  - Select either *sp1*, *sp2*, or *sp3* from the target devices menu.
  - Select *Enable native IP* from the list of management actions the user is authorized to perform on the target device.

    -or-
  - Enter **ssh** to execute the **nativeipon** command directly using the target device alias:

    ssh *username*:*device_alias*@**172.20.0.1 nativeipon**

Accessing native features for example 3

After enabling native IP access, the user can access one of the desired native features that may be available on the target device, including:

- A native web application, which the user may access in one of the following ways:

- In the Web Manager on the SP manager, the user selects the *Go to native web interfac*e link on the Access Target Devices screen.
- On the user's workstation, the user enters the virtual IP address of the target device in a browser.
- On the user's workstation, the user enters the **ssh** command on the command line with the name/alias of the target device along with the virtual IP address of the SP manager.

  For example, the following **ssh** command line entered by the user named **allSPs** accesses **sp2** using the SP manager's virtual IP address **172.20.0.1**.

  ```
  ssh -t allSPs:sp2@172.20.0.1
  ```

- A management application, which the user may access in one of the following ways, depending whether the application is a client on the user's workstation or resides on the SP:
  - If the management application resides on the user's workstation, the user brings the management application up from the workstation.
  - If the management application resides on the SP, and is an executable that can be invoked on the command line, the user accesses the SP's console first in one of the following two ways:

    The user enters **ssh** with the **spconsole** command in the following format:

    ```
    ssh -t allSPs:sp2@172.20.0.1 spconsole
    ```

    -or-

    In the Web Manager on the SP manager, the user clicks the *SP Console* link on the Access Target Devices screen.

    After accessing the SP console, the user launches the management application from the SP's command line.

Options for assigning IP addresses to target devices

After the addressing scheme is planned as described in *Address configuration for target devices* on page 180, the administrator must do both of the following:

- Assign an IP address in the planned range of addresses when configuring each target device on the SP manager, as described in *Parameters for configuring target devices* on page 47.
- Assign the same IP address on the target device itself.

The available options for assigning IP addresses on the target devices are summarized in the following bulleted list:

- A target device may have a default IP address already assigned.

  In most cases, such a default IP address would not be used. Instead an IP address of the administrator's choosing would probably be assigned from the site's private-side target device IP addressing scheme, using one of the other available methods.
- The administrator may directly configure a target device with a static IP address.

Configuration of a target device's static IP address would be done using whatever means are available (such as an SP's console port, the server's firmware setup, or software running on the server).

- If target devices are running DHCP client software, then the administrator can assign the desired fixed IP address to the target device's MAC address in the dhcp.conf file, as described in *Configuring the DHCP Server* on page 120.

Appendix D: Advanced Boot and Backup Configuration

Boot file location

How the MergePoint 5224/5240 SP manager boots is introduced at a high level in *Configuring Boot Characteristics* on page 75 in the section on configuring boot in the Web Manager. The additional information in this section is to give an administrator who has the root password enough background to be able to boot from an alternate image if the need arises and if the Web Manager is not available.

The MergePoint 5224/5240 SP manager uses a U-Boot boot loader that resides in soldered Flash memory and that automatically runs at boot time. U-Boot boots the SP manager from an image whose location is configurable. The image can reside either in a separate removable Flash memory on the SP manager or on a boot server on the network.

Up to two images may be stored at the same time on the SP manager's removable Flash. Each image on the removable Flash has three separate file systems mounted on three Linux partitions. The first partition for each image contains the kernel, the second partition contains the root filesystem mounted read only and the third partition contains the configuration files mounted read-write.

See http://sourceforge.net/projects/u-boot. for more about U-Boot in general.

The SP manager boots from alternate images as described below.

- The SP manager initially boots from a software image referred to as image1, which is stored in three partitions on the removable Flash (hda1, hda5 and hda7).
- The first time you download and install a new software version from Cyclades, the new image is stored as image2 in another set of three identical partitions on the removable Flash (hda2, hda6, and hda8), and the configuration is changed to boot the SP manager from image2.
- The second time you download a new software version, the latest image is stored as image1 in the first set of three partitions, and the SP manager configuration is changed to boot from image1.
- Subsequent downloads are stored following the same pattern, alternating image1 with image2.

Refer to the following text and figure explaining partition numbers if needed for understanding the instructions about boot configuration. As illustrated in the following figure, the first partition for each image contains the Linux kernel, the second partition contains the root-mounted filesystem (which is mounted read only), and the third partition (which is mounted read write) contains the configuration files.

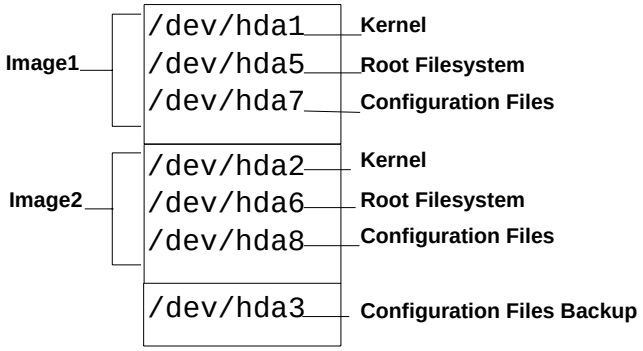

Figure D.1: Boot Partitions

The previous figure also shows a configuration backup partition (/dev/hda3 in removable Flash). This partition is mounted as /mnt/hda3. The /mnt/hda3/backup directory is used for storing compressed copies of backed-up configuration files, as shown in the following screen example.

```
[root@MergePoint5224 root]# cd /mnt/hda3/backup
[root@MergePoint5224 backup]# ls
configuration_files.gz
```

Downloading a new software version

You can download a new software version in the following ways:

- Use the Web Manager Mgmt - Firmware Upgrade screen to download the image from an FTP server.

  When the image is downloaded by FTP, a script (saveimage) automatically extracts the filesystem from the image, mounts it and copies the files to the removable Flash. Since the current image is being run from one of the three-partitions sets, the downloaded image is stored in the other set of three partitions. The environment variable currentimage is changed so that the system boots from the new image.

- Do a network boot from the image and then save it onto the removable Flash.

  The U-Boot monitor command net_boot boots the image from the TFTP server specified in the environment variables. After the image is downloaded by network boot, the root filesystem is in the RAMDISK, and the image can run even if no removable Flash card is inserted.

  From the command line, you can then run the create_cf script with the --doformat option to automatically save the image from RAMDISK into the removable Flash. The script erases everything in the Flash, partitions the Flash, if necessary, formats the partitions and copies the files currently in the RAM into the corresponding image partitions. If the Flash is already partitioned, you can choose where the image is saved using the option --image<N>.

Changing the boot image

If you want to change to another image from the current one, and if you have access to the Web Manager, you can use the Config - Boot Configuration screen to select the other image and then use the Restart button on the Mgmt - Restart screen to boot the SP manager from the new location.

You have two other options if you cannot access the Web Manager:

- Use the cli utility

  See *To use the sptemplate utility to test a template:* on page 179.
- Boot in U-Boot monitor mode and use the available boot commands

  See *To use the sptemplate utility to test a template:* on page 179.

To boot from an alternate image using cli:

1. Connect to the SP manager from a terminal connected to the console port or create a telnet or ssh connection, and log in as **root**.
2. Enter the **cli** command.

   ```
   # cli
   ```
3. Enter **get bootconf** to check the current configuration to find out which boot command and boot image are being used.

   In the screen example, hw_boot is defined as the bootcmd and image2 is defined as the image.

   ```
   cli> get bootconf
   ...
   bootconf bootcmd: hw_boot
   ...
   bootconf image: 2
   ```
4. To boot from a TFTP boot server over the network, perform the following steps:
   a. Set the value of **bootconf bootcmd** to **net_boot**.

      ```
      cli> set bootconf bootcmd net_boot
      ```
   b. Set the value of **bootconf serverip** to the TFTP boot server's IP address.

      ```
      cli> set bootconf serverip IPaddress
      ```
   c. Set the value of **bootconf bootfile** to be the name of the boot file on the TFTP server.

      ```
      cli> set bootconf bootfile allImage.0830 IPaddress
      ```

   The currentimage environment variable is changed to boot from the specified image.

Changing the boot image in U-Boot monitor mode

You can access U-Boot monitor mode in one of the following two ways:

- During boot, when the Hit any key to stop autoboot prompt appears, pressing any key before the timer expires brings the SP manager to U-Boot monitor mode.
- If boot fails, the SP manager automatically enters U-Boot monitor mode.

The U-Boot hw_boot command boots from either the first or second image according to the value of the currentimage environment variable. You can use the following procedures to change which image is used for booting.

To boot in U-Boot monitor mode:

1. Access the SP manager command line and log in as root.
2. Enter the **reboot** command.

   ```
   # reboot
   ```

3. During boot, when the Hit any key to stop autoboot prompt appears, press any key before the time elapses to stop the boot. The U-Boot monitor prompt appears.

   ```
   =>
   ```

4. Enter **help** to see a list of supported commands.

   ```
   => help
   ```

To boot from an alternate image in U-Boot monitor mode:

1. Go to U-Boot monitor mode.
2. Set the **currentimage** environment variable to the number of the image you want to boot.

   ```
   => setenv currentimage N
   ```

   For example, to boot from image2 enter **setenv currentimage 2**, as shown in the following screen example.

   ```
   => setenv currentimage 2
   ```

3. Enter the **hw_boot** command.

   ```
   => hw_boot
   ```

To boot in single user mode from U-Boot monitor mode:

1. Boot in U-Boot monitor mode. If needed, see *To boot in U-Boot monitor mode:* on page 203.
2. Boot in single-user mode by entering **hw_boot single**, as shown in the following example.

   ```
   => hw_boot single
   ```

The single-user prompt appears, as shown in the following example.

```
[root@(none) /]#
```

U-Boot network boot options and caveats

When a network boot is performed with the U-boot net_boot command, the SP manager boots from the specified image on the TFTP server. The image uses the RAM as the root file system. Network boots are useful for troubleshooting because the net-booted image can run even if the SP manager's Flash memory is not usable.

Network boots are recommended only for troubleshooting and must not be used for normal operation of the SP manager. For example, if you want to test a new release of the software to make sure a problem is fixed, or if the removable Flash memory becomes corrupted, you could download the software to a tftpboot server and then save it to the removable Flash after testing, using the create_cf command with the appropriate options (see *Options for the create_cf command* on page 205).

When a network boot is performed, the system uses one of the two following sources of configuration data:

- If the net_boot command is entered with the configsource=factory_default option, the factory_default configuration files are loaded.
- Otherwise, the backed up configuration files from the /dev/hda3 backup partition are copied to the RAMDISK and used.

Any configuration changes made after the last backup copy was made are lost unless the configuration files were backed up before the network boot and then restored afterwards (see *Backing Up Configuration Files* on page 129 and *Restoring Backed Up Configuration Files* on page 129).

To upgrade to a boot image from a network boot:

Before performing this procedure, make sure that a copy of the latest boot image has been downloaded from the Avocent ftp site to a TFTP server that is accessible to the SP manager.

1. Boot in U-boot monitor mode. If needed, see *To boot in U-Boot monitor mode:* on page 203.
2. Use the **setenv** command to set the **ipaddr**, **serverip** and **bootfile** environment variables.

   ```
   => setenv ipaddr SPmanager_IPaddress
   => setenv serverip boot_server_IPaddress
   => setenv bootfile boot_filename
   ```

   The format of the boot filename is: **fl**<seven_digit_version_number>**.bin**. In the following example, the filename **fl2222222.bin** is used,

   ```
   => setenv ipaddr 192.168.45.29
   => setenv serverip 192.168.45.127
   => setenv bootfile fl2222222.bin
   ```

3. Check that the environment variables are set properly with the **printenv** command.

```
=> printenv
ipaddr=192.168.45.29
serverip=192.168.45.127
bootfile=fl2222222.bin
```

4. Enter the **save** command.

```
=> save
```

5. Enter the **net_boot** command.

```
=> net_boot
```

6. Log in as **root** after boot completes.
7. Unmount **/dev/hda3**.

```
[root@MergePoint5224 /]# umount /dev/hda3
```

8. Run the **create_cf** command with the **--doformat** option.

   The following command example shows entering the **--factory_default** argument to restore the factory default configuration files at the same time.

```
[root@MergePoint5224 /]# create_cf --doformat --factory_default
```

CAUTION: Be aware that the --doformat option erases the Flash memory and installs the boot image into the image1 area. See *Options for the create_cf command* on page 205 for other options.

   The following text appears when the operation completes.

```
Creation of image <N> completed.
...
```

9. Enter the **reboot** command to restart the unit.

```
[root@MergePoint5224 /]# reboot
```

Options for the create_cf command

Administrators can use the create_cf command when troubleshooting problems with the boot image, as described under *To upgrade to a boot image from a network boot:* on page 204. Use it carefully as described in this section.

CAUTION: Only use the --doformat option to save the image that is currently in RAM into the image1 area, but be aware that this option reformats all Flash partitions while saving the image.

NOTE: Use the --image[1|2]option to save the image that is currently in RAM into a specific image area, without reformatting the partitions that contain the other image.

Table D.1 provides more information about the create_cf command options, which you can view from the Linux command line by entering the name of the command.

Table D.1: Options for the create_cf Command

Option	Description
none	Not recommended. Checks if a boot image is already on the target device. If no image is on the target device (as would be true for a newly installed removable Flash on a PC card) and if no image is specified, runs --doformat and installs the image in image1. If multiple images are on the target device, and no image is specified, presents a choice of images for the user to choose from, and then writes the image from RAM into the specified image area. In either case, restores the factory default configuration.
-d device	Creates the image on the specified device (the default device is /dev/hda - the removable Flash memory). Used to create the image in another location, such as on an installed compact Flash PC card. Device names for PC cards are determined by the number of the card slot where the card is installed, either /dev/hdc (PC slot 1) or /dev/hde (PC slot 2). **NOTE:**Before using, make sure the filesystem is not mounted.
--factory_default	Creates the image using factory default configuration files. By default, if this option is not entered, the configuration from the current partition is used, if valid. For more details, see *How Configuration Changes Are Handled* on page 55.
--doformat	Rebuilds the partitions, erasing their contents. Creates the image as image1.
--dontformat	Does not format the compact Flash. The sizes of partitions hda1-3 and 5-8 are checked. If the partition sizes are not smaller than 2, 2, 5, 51, 51, 6, and 6 Mbytes respectively, the image is installed in the specified image area.
--imageN	Creates/replaces imageN, when n=1 | 2. Use this option to replace only the specified image without erasing both images. Changes the currentimage environment variable to boot from the image.

Examples for create_cf command usage

Both examples assume you have done a network boot and you want to save the boot image from RAM.

To save a boot image to a compact Flash PC card:

1. Perform a network boot.
2. Insert a compact Flash PC card into a card slot.
3. Enter the following **create_cf** command line to save a copy of the image from RAM onto the card. The compact Flash card in the example is inserted into slot 1.

```
[root@MergePoint5224 /]# create_cf -d /dev/hdc --image1
```

4. Enter the **reboot** command to restart the unit.

```
[root@MergePoint5224 /]# reboot
```

To save a boot image into the Image2 area and restore the factory default configuration:

1. Perform a network boot.
2. Unmount the resident removable Flash memory.
3. Enter the following **create_cf** command line to save the image from RAM and restore the factory default configuration.

   The example shows saving the image into the image2 area.

```
[root@MergePoint5224 /]# create_cf --factory_default --image2
```

4. Enter the **reboot** command to restart the unit.

```
[root@MergePoint5224 /]# reboot
```

Options for the restoreconf Command

You may need to use the restoreconf command while troubleshooting. All the restoreconf subcommands are shown in the following screen example.

```
restoreconf:
Usage:
Restore from Flash:           restoreconf
Restore from factory default: restoreconf factory_default
Restore from storage device:  restoreconf sd
Restore from local file:      restoreconf local <FILE>
Restore from FTP server:      restoreconf ftp <FILE>
<FTP_SERVER> <USER> <PASSWORD>
Restore from TFTP server:     restoreconf tftp <FILE>
<TFTP_SERVER>
Restore from SSH server:      restoreconf ssh <FILE>
<SSH_SERVER> <USER>
```

Appendix E: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating issues you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service.

To resolve an issue:

1. Check the pertinent section of this manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the online service request.
3. Call the Avocent Technical Support location nearest you.

INDEX

Numerics

1U device 1

A

Active Directory schema, configuring 134
adding rules for IP filtering chains 54
addressing scheme for device
  introduction 46
addressing scheme for devices
  planning 63
administrative users
  adding rules to packet filtering chains 102
  admin group, assigning on an authentication server 133
  configuring in Web Manager 81
  configuring notifications, alarms, and email 44
  configuring SNMP 96
  features of Web Manager screens 12, 58
  two types of access to Web Manager 57
  Web Manager administration 21
administrators 16, 57
ADSI Edit 134
AH authentication protocol 34
alarms
  configuring 43, 44
  IPDU 4
  triggers, configuring
    email notifications 93
    pager notifications 92
    SNMP trap notifications 91
ALERT syslog severity level 38
alias
  hostname
    cli parameter example 150
    cli parameter, automatic deletion of 153
    configuring for DHCP 121
    parameter, automatic creation of 150
    using cli utility 160
  target device 47, 113
    configuring in cli utility 150
ALOM 48, 170
anonymous logins to Cyclades' ftp server 108
Apache web server, restarting 119
authenticated users 33
authentication
  configuring
    for connected devices 10
    for the SP manager with cli 158, 162
  supported methods
    for the SP manager and connected devices 22
    IPSec 34
authentication methods
  introduction 22
  AH 34
  default, defined in Moderate security profile 26
  group authorizations configurable with 133
  LDAP, RADIUS, TACACS+, configuring group authorizations with 133
  OTP introduction 24
authentication servers
  configuring
    LDAP 86

authentication servers (Continued)
NIS 87
RADIUS 87
SMB 88
TACACS+ 89
authorized users 33
accessing devices through the SP manager 21
and Expect scripts 169
bypassing authorizations per custom security profile 26
VPN configuration tasks 34, 36
autodetect modem access type 42
AUX ports
illustrated 2
LEDs 3
Avocent
downloading appliance firmware updates from 109
downloading IPDU firmware updates from 68
firmware download ftp password 108

B

backing up configuration files 129, 130
backup partition 201
baud rate, modem 42
/bin/do_create_cf_ext2 script 114
blade managers, connecting 10, 39
bond0 39, 40
boot
action, configuring for IPSec VPN 35
configuration fields and options 76
configuring in Web Manager 77, 78
boot image
checking if one exists 206
locations 200
partition locations 201
problems, troubleshooting 205
replacing 167, 200
saving to compact Flash PC card 206
troubleshooting problems with 167
brackets, mounting 8
broadcast IP address 41, 102
browser 15
buttons
save and apply changes 129
unsaved changes 128

C

CA
See certificate authority
cabinet mounting 9
cables
connecting 8
DB-9 female to RJ-45 8
RJ-45 to DB-9 13
RJ-45 to RJ-45 Ethernet CAT5 9
callback
configuration option 42
connection, used for troubleshooting 165
using to access the Web Manager 57
Cautions
changing admin passwords 61
closing PPTP VPN connections to prevent unauthorized access. 37
complying with FCC and CE certification requirements 10
create_cf --doformat option 205
device IP address visibility 192
disabling native IP before ending PPTP VPN connection 37

Cautions (Continued)
Kerberos time/date synchronization requirements 84
network boot image 205
OTP 116
private subnet requirements for devices 65, 79
risks from not changing administrator's passwords 61
safety precautions 8
shielded cable requirements for compliance with FCC and CE requirements, 168
using snmpd without a VPN tunnel 30
when changing or deleting private subnets 64, 106
when changing the default rmenu.sh menu 126
when creating a command template 179
when creating filtering rules 53
certificate signing request, generating 119
chains, packet filtering 53
circuit breakers 10
cli utility
add command 149, 152
adding a user 117
commands 149
commit command 153
configuring
alarms 43, 44
authentication 24, 53
basic network parameters 13, 14
modems 41, 42
rules for IP filtering 53
services 27
users 25
delete command 153
detecting services starting and stopping 27
enabling data buffering 52
exit command 154, 155
list command 155
quit command 155
quit! command 156
rename command 156
revert command 156
saving (committing) changes 53, 129
set command 157
shell command 157
show command 154
using to enable Web Manager access 12
version command 157
command line
using ssh command on to access the SP manager 36
using to check for the PPTP address 37, 190, 196
command templates
creating 169
table showing devices to which they apply 173
when not to assign to devices 50
commands
cli utility 24, 25, 53, 129
enabling data buffering 52
commit 129
create_cf utility 167, 205, 206
httpd -k 167
ifconfig 190
ipconfig 37, 196
ipmitool 50
openssl 119
opiekey 117, 118
opiepasswd 117, 118
ping 178
ps 167

commands (Continued)
restoreconf 130
saveconf 129, 179
sptemplate utility
introduction 174
testing a template 179
using to create a new template 178
when to use 173
ssh 36, 178
telnet 178
using for troubleshooting 206
communications
blocked between private Ethernet ports 39
proxied 21
compact Flash PC card
saving the boot image on 206
using to mount the /mnt/opie directory for OTP support 114
configsource environment variable 204
configuration 12
boot 76
files 129
backed up 129, 201
factory default 55, 207
restoring to factory defaults 130
saving changes 128
source of data during a network boot 204
configuration_files.gz backup file 129
connecting cables 8
console
accessing through dedicated Ethernet ports 45
accessing to restore factory defaults 130
destination for syslog messages 38
logout 179
console access 15
console cli parameter 163
console port 12, 13, 14, 15
LEDs 3
create_cf command 205
options 206
using to replace a corrupted image 204
using when troubleshooting 167
CRIT syslog severity level 38
crond daemon 43
currentimage environment variable 201, 206
custom security profile
with the override authorizations feature set 26
customizing
command templates 174
expect scripts 174
Cyclades PM IPDUS
downloading software for 68
overcurrent status generating syslog messages 38

D

daemon.sh command, WEB option 167
daemons 43
daisy-chaining Cyclades PM IPDUs 19
data buffering
introduction 22, 52
configuring with cli 162
configuring with Web Manager 79
options for devices 48
data filtering, events generating syslog messages 38
date and time, configuring 74
DB-9 female to RJ-45 cable 8
DB-9 male COM port 13
DC models 11
DEBUG syslog severity level 38

dedicated Ethernet ports 45
default route 43, 62
  specifying 102
  when private subnets are not configured 64, 106
defaults
  configuration files 207
    restoring 130
  data buffering, configuring 52
  IP addresses
    using to access the Web Manager 15
  packet filtering chains 53
  SP manager IP address, using to access 13
  static IP address 101
Destination Network Address Translation
  See DNAT
/dev/hdc PCMCIA slot 1 device name 206
/dev/hde PCMCIA slot 2 device name 206
devconsole 170
devconsole.default command template 173
devices
  See target devices
DHCP 12
  configuring
    in Web Manager 101
    in Wizard 62
    notes 41
  default route, automatically assigned by DHCP server 43, 62
  when the server cannot be reached 101
DHCP server 12, 14
dial-ins 57
  introduction 41
  configuring OTP authentication for 115
DirectCommand 38, 131, 164, 170
  introduction 38
  compared to Native IP 33
  troubleshooting 165
directcommand 38
directcommand cli parameter 163
directcommand_only 48
DNAT 63
DNS
  configuring in Web Manager 102
  name 12
do_create_cf_ext2 script 114
domain name 102
downloading
  firmware (software)
    Cyclades PM IPDU 68, 109
    SP manager 68, 109
DRAC device
  family 170
  type command template 173
drac.default command template 173
dynamic IP address 14

E

edit rule for packet filtering chain 54
email address, configuring for system email 77
email notifications, configuration options 44
EMERG syslog severity level 38
encrypted communications 33
encryption 33
environment variables, currentimage 206
ERROR syslog severity level 38
ESP authentication protocol 34
/etc/config_files
  adding a new file to be backed up/restored 130
  certificate files pre-added to 120
/etc/httpd/conf/ssl.key/server.key file 119

/etc/mgetty.login.config file 115
/etc/pam.d/login file 115
/etc/pam.d/otp file 115
/etc/pam.d/otplocal file 115
/etc/pam.d/sshd file 115
/etc/raddb/server file 137
eth0 and eth1 40
Ethernet
  cable 9**,** 10
  failover 9
  PC cards
    connecting 9
    eth2 and eth3 interfaces 39
    using and configuring 9
Ethernet interfaces
  configuring specific speeds 40
Ethernet ports
  introduction 39
  configuring a static IP address for 102
  configuring, Web Manager 101
  private 2**,** 10
examples
  private subnet configuration 184
  two private subnets and VPN 185
  virtual network configuration with one private subnet 193
Expect scripts
  arguments 170
  exit codes 172
  using 169
  when a customized one is needed 173
external modems 41
  connecting 4

F

factory default configuration files
  how stored and restored 55
  restoring
    overview 55
    with the command line 130
    with the create_cf command 206
    with the create_cf command, example 207
    with the restoreconf command 130
failover 9
  introduction 39
  configuration, Wizard 62**,** 63
  configuring 102
family, device 170
figuring 39
files
  configuration_files.gz 129
  /etc/config_files
  /etc/httpd/conf/ssl.key/server.key file 119
  /etc/mgetty.login.config file 115
  /etc/pam.d/login file 115
  /etc/pam.d/otp file 115
  /etc/pam.d/otplocal file 115
  /etc/pam.d/sshd file 115
  /etc/raddb/server 137
  hdc.conf 84
  /mnt/hda3/backup/configuration_files_gz file 129
firewall
  configuration introduction 53–55
  rules, configuring, Web Manager 102
firmware
  Cyclades PM IPDU, downloading 68
  image 206
  SP manager, downloading 68**,** 109

Flash memory
PC card 206
saving the boot image on 206
SP manager, unusable, recovering from 204
SP manager removable
partitions 205
upgrading firmware on 109
flow control 42
format storage media, while creating a boot image 206
FORWARD packet filtering chain 53
FTP
site for downloading SP manager firmware 108

G

gateway
configuring in Web Manager 102
configuring in Wizard 41
grounded wire 11
groups
authorizations, configuring on authentication servers 133
configuring with cli 162
configuring with Web Manager 81

H

hdc.conf file, on the Kerberos KDC 84
hex screw 11
high-availability 39
host route 43
HTTP 26, 57
HTTPS 26, 28, 57

I

ICMP 26
ifconfig command 37, 40, 190, 196
iLO
device family 170
devices, default command template for 173
ilo.default command template 173
image, software 206
info attribute, configuring on a Active Directory server 134
INFO syslog severity level 38
INPUT packet filtering chain 53
installation
advanced 17–19
basic 7–16
interfaces
See also network interfaces
Internet access 9
intrusion, reducing risks of 61
inverted options for packet filtering 55
IP addresses
broadcast 102
configuring for Web Manager access 12
default 15
DHCP, to access the Web Manager, using 14
dynamically assigned 15
of remote IPSec gateway 35
planning 63
IP filtering, introduction 53–55
IPDUs
See Cyclades PM IPDUs
IPMI 1.5 target devices
command template requirements 173
configuration type 48
family 170
IPMI 2.0 48, 170
ipmitool command 50

IPSec
authentication methods 22
in the Moderate security profile 26
VPN configuration tasks 36
iptables introduction 53–55

K

Kerberos authentication method 22, 34
Key Distribution Center (KDC) 84
keys generated for RSA public keys 34

L

LAN, connecting the primary Ethernet port to 9
LDAP authentication method
introduction 23
configuring for OpenLDAP server 133
configuring for Windows Active Directory 133
configuring group authorizations with 133
configuring in Web Manager 85, 87
VPN configuration exclusion 34
LEDs 3
lightweight directory access protocol
See LDAP
Linux operating system
command line, viewing create_cf options on 206
configuring PPTP on 36
support for IPSec and PPTP on 34
local
administrators, troubleshooting 165
authentication 22
fallback options 22
local area network
See LAN
logging, system 22
login shell 43, 126
logins
anonymous to ftp.cyclades.com 108
authentication options for 22
modem access type 42
name and password for a target device 48

M

MAC address 39
Macintosh
creating PPTP VPN connections from 36
MacOS X support for IPSec and PPTP 34
maintenance tasks not done using Web Manager 111
management features 33
management network, connecting to 39
management of connected devices 21
MergePoint 5224/5240 SP manager
1040 DAC model 1
features overview 21
administrator 174
configuring a default route 43, 62
granting access to VPN connections 33
IP address for the public interface 37
mounting brackets 8
requirements for device configuration 169
system events generating syslog messages 38
to rackmount 9
understanding authentication on 22
web server 119
message filtering
levels, syslog 38
message logging 38–39
MindTerm applet console connection 113
/mnt/hda3/backup directory 129
/mnt/hda3/backup/configuration_files_gz file 129
/mnt/opie directory 114

modems
access type menu options 42
external 41
initialization string 42
introduction 41–42
tasks for configuring 41
types 4
used for troubleshooting 165
mounting
brackets 8
SP manager 9
MS-CHAPv2 34
MTU 41, 102

N

name, target device 47
native IP
command template for any device type 173
configuring access
through PPTP VPN tunnel 36
enabling
after creating PPTP VPN tunnel 37
after VPN tunnel is created 36
starting the VPN connection from a remote computer 34
nativeip 163
nativeipon 33
nci cli parameter 163
net_boot command 201
netmask
for IPSec VPN connections 35
for SP manager 102
network
boot 204
configuration, checking for trouble 178
network interfaces
configuring 101
a default route 43, 62
Wizard 62, 65
network route 43
network services 27
NIS authentication server
configuring 86, 87, 88, 89, 91, 92, 93
Notes
/usr/sbin/ directory mounting 111
accessing an SP's console to find command syntax 178
adding groups to a Frame-Filter-Id definition 137
adding users 118
arbitrary assignment of PPTP IP address pools 189
cli utility not displaying OTP authentication 116
configuration is per device not per port 107
configuring
a user as an administrative user on an LDAP server 134
authentication 10
groups on a RADIUS server 139
configuring groups on a TACACS+ authentication server 140, 141
configuring services 27
configuring the secondary Ethernet port 63
configuring users for PPP/PPTP 190
configuring users on an LDAP server for group access 135, 136
connecting to an SP's console 178
daisy-chained IPDUs running the same firmware 19
daisy-chaining IPDUs 68
DHCP configuration of IP addresses 29

Notes (Continued)
effects of selecting a default authentication type 26
handling unsupported sensors in command templates 179
HTTP disabled in secured profile 100
invoking ssh with the -t option 171, 172
IP address used for the SP manager's default route 102
IPDU master and slave units 70
Kerberos requirements for time and date synchronization 85
login session time-outs 57
losing configuration file changes 153, 155
modem configuration with cli 41
not all cli parameters and values described 143
not using cli user to configure new users 152
OTP authentication support 73
OTP secret pass phrase 118
PC cards occupying two card slots 17
powering the SP manager 19
powering with separate power sources 10
saving server.key and server.crt files 120
saving the image from RAM 205
setting a gateway IP address and a default route 127
slapd.conf file location on LDAP server 135
SNMP and the security profile 96
storing buffered data in separate files 113
testing access to the SP manager 188
unique device configuration requirements 169
users and groups on TACACS+ servers 140
using a crossover cable for terminal connections 13
using talk_customN.exp scripts 172
using the default IP address 15
virtual network addresses unsupported 192, 194
virtual network advantages 36
Web Manager support for OTP authentication. 115
workaround for packets blocked by a firewall 188
NOTICE syslog severity level 38
notifications
configuring 44
in security features table 22
notifications of over-current states 4

O

off-the-shelf cables 9
one time passwords in everything
See OPIE
OpenLDAP authentication server 133
openssl utility 119
OpenSWAN 34
opiekey command, generating passwords for users 117, 118
opiepasswd command, registering users 117, 118
OTP authentication method
introduction for administrators 24
for dialing into PC modem or phone cards 42
generating passwords for users 117
OTP/Local 115
where supported 23
registering users 117
specifying the databases' location 114
where supported 23
outlets, configuring 4
OUTPUT packet filtering chain 53

P

packet filtering
introduction 53–55
on the SP manager 53
overview 53
rules 54
pager notifications 44
partitions
checking partition size with create_cf 206
rebuilding 206
reformatting with create_cf 205
passwd command 14
passwords
administrative user 12
changing one's own 57
changing root's 15
root user, changing 15
target device 48
PC cards
and create_cf 206
compact Flash
configuring 74
saving the boot image on 206
Ethernet
configuring 73, 74
connecting 9
Flash memory, saving the boot image on 206
modem
beginning to configure 72
configuring 72
overview 41
modem, connecting 4
PCMCIA slots 1
Phillips screwdriver 8, 9
ping command 178
planning device IP addresses 63
positive wire to DC power 11
power cli parameter 163
power cords 10
power management
commands 169, 178
daisy-chaining Cyclades PM IPDUs 4, 19
power on 169
power sources 11
power switches 10, 11
PPP
authentication 22
modem access type 42
user configuration settings 25
using to access the Web Manager 57
PPTP 22, 25, 26, 34
client 34, 37, 190
password 37
VPN connections 36
pptp-linux 34
preshared key (PSK) 34
primary Ethernet port 9, 45
priv0 39, 182
private Ethernet ports 2, 10, 45
private network 21, 39
private subnets
caution when changing or deleting 64, 106
configuration example 184, 185
configuring, Wizard 63
device configuration task 169
protocols, vulnerabilities not exposed on public network 21
proxied communications 21
ps command 167

PSK (preshared key) 34
public key
SSL 119
SSL certificate request 119
public network 21, 39

Q

Quick Start Guide 8

R

rackmounting 8, 9
RADIUS authentication method
introduction 23
configuring group authorizations with 133
configuring in Web Manager 87
for PPTP VPNs 34
RAM
root filesystem in after network boot 201
saving an image to Flash 109
used to store a network boot image 201, 204
used to store changes until they are saved 55
redundancy 10
remote administrators, troubleshooting 165
removable Flash 201
restart
dhcpd, for enabling DHCP target device address management 122
LDAP for enabling groups on the LDAP server 135
persistence of configuration file changes after 55
syslog-ng, for putting syslog-ng.conf file changes into effect 112
to boot SP manager from a new location 202
web server, for putting a security certificate into effect 120
web server, when Web Manager stops responding 167
restoration
configuring for added files 130
tasks for configuration files 129
restoreconf command
factory_default option 130
options 207
restoring
backed up configuration files 55
factory default configuration files 55, 130
RJ-45 to DB-9 6 ft. CAT5 cable 13
RJ-45 to RJ-45 Ethernet CAT5 cable 8, 9
rmenush login shell 43, 126
configuring 43, 126
root user
changing the password 15
changing the user console login menu 126
routers 9
routing
for the SP manager, understanding 43
specifying the SP manager's default route 43, 62
RSA II devices
default command template for 173
differences between devices of the same type 169
family 170
RSA public keys 34
rsa.default command template 173, 178
rsa.limited.default command template 173, 178
RTN screw 11
rules
configuring for packet filtering 53
hidden, for packet filtering 53
packet filtering 54

S

safety precautions 8
save and apply changes
button 129
using the cli utility 129
Save button on the Mgmt-Backup/restore screen 129
saveconf command
backing up configuration changes 129
run as prerequisite to restoring backed up configuration files 129
saving a newly configured template 179
saving configuration file changes
procedures 128
screwdriver 8
screws 8, 9
scripts
configuring backups for 130
Expect
how used for device communications 169
arguments 170
exit codes 172
secondary Ethernet port 9, 39
security
changing admin user password 61
isolating devices from the public network 39
security profiles
configuring on a new MergePoint 5224/5240 SP manager 16
effect on authorizations 25
selecting or customizing, Wizard 61
security tunnel 33
sel cli parameter 163
self-signed certificates 28
sensors
alarms
configuring 43, 44, 93
events generating syslog messages 38
sensors cli parameter 163
servers
authentication, configuring
LDAP 86
NIS 87
RADIUS 87
SMB 88
TACACS+ 89
syslog 39
service processors 10
connecting multiple to a single private Ethernet port 39
connecting to the SP manager
illustrated 45
multiple to a single private Ethernet port 39
console 178
access usually available 178
hiding vulnerable protocols used by 21
types 48
services
administration options described 27
controlled by security profiles 26
shared secret 34
shipping box contents 8
SMB authentication method 24
SMB authentication server, configuring, in Web Manager 89, 90, 93, 94, 95, 96
SMTP server, configuring for system email 77
SNMP
security profile configuration 26
trap notifications 44
v1, v2, v3 29

software
downloading
Cyclades PM IPDUs 68
for the SP manager 108, 109
image
saving from RAM to Flash using create_cf 206
upgrading
retaining configuration file changes 55
spmanager cli parameter 163
spmanager user 25
SPs
See service processors
sptemplate utility
introduction 174
procedure for using 178
use by the administrator 173
using to test a template 179
SSH
configuring OTP authentication for 115
enabled in moderate security profile 26
encryption 21
in MindTerm 113
tunnel
creating with a MindTerm applet 113
tunnel, administrative user creating using MindTerm 113
ssh command 36, 37, 178, 190, 196
alias for target device 47
nativeipon 33
SSL certificate requirements 28
static IP address 34, 102
configuring for Ethernet ports
Web Manager 101
subnets
configuring in Wizard 63
for IPSec VPN connections 35
switch 9, 10
syslog
introduction 38–39
message filtering levels 38
message logging with 38
message notifications 44
servers 38, 39
severity levels 38
syslogd 39

T

TACACS+ authentication method 24, 34
configuring group authorizations with 133
TACACS+ authentication servers
configuring in Web Manager 89
talk_alom.exp Expect script 170
talk_devconsole.exp Expect script 170
talk_DirectCommand.exp Expect script 170
talk_drac.exp Expect script 170
talk_ilo.exp Expect script 170
talk_ipmi_1.5.exp Expect script 170
talk_ipmi_2.0.exp Expect script 170
talk_rsa_II.exp Expect script 170
target devices 10, 14, 21
accessing native IP features on 33, 36
alias 47
assigning an authentication method to with vi 116
assigning private subnets to 50
configuring 16
configuring VPN for Native IP access 33
connecting 45

target devices (Continued)
console access through dedicated Ethernet ports 45
default authentication method 26
defining families 170
management 21
management actions 47
name 47
types 48
target devices groups, assigning to devices 48
tasks
for basic configuration, Wizard 60
for configuring
IPSec VPN 36
native IP access 36
PPTP connections and native IP 37
PPTP VPN connections 36
VPN 36
not doable using Web Manager 111
TCP ports and DirectCommand 165
Technical support 208
Telnet 26**,** 130
telnet command 178
terminal 13
Terminal Access Controller Access Control System authentication
See TACACS+
terminal emulation program 13
terminal emulator 41
TFTP boot server 204
trap notifications 44
troubleshooting 165–167
boot image problems 167**,** 205
connection methods 165
DirctCommand fails 165
network boots and 204
network failure 165
understanding boot for 200
Web Manager stops responding 167
tunnel 33
type
device 48
types of target devices 48

U

U-Boot
introduction 200
monitor mode 204
UNIX-based servers 39
unsaved changes
button 128
user accounts 25
username for Cyclades ftp site 108
users 14
adding 16
configuration options 25
configuring
in Wizard 66
/usr/bin/rmenush login shell
configuring 43**,** 126

V

virtual IP addresses
assigning to a new device 169
virtual network
configuration in Wizard 63
VPN
introduction 33–37
configuration example 185
connections

VPN (Contineud)
IPSec 122
PPTP 36

W

WARNING syslog severity level 38
Web Manager
accessing for configuration 14
enabling access 12
not displaying OTP authentication 116
procedures for enabling access to 13
restarting 167
to use a dynamic IP address to access 14
to use the default IP address to access 15
using 57–110
web server
Apache 119
replacing autogenerated SSL certificate in 119
web server restart 119
Windows
Active Directory server, configuring for group authorizations 133
Administration Pack, installing 133
and PPTP VPN connections 36
support for IPSec and PPTP 34
wire, grounded 11
Wizard 60–67

X

X.509 certificates 34

Avocent®

The Power of Being There®

For Technical Support:

www.avocent.com/support

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201
USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Canada
20 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1K3 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99

590-679-501A